SAFETY ANALYSIS OF SAFETY PARAMETER DISPLAY SYSTEM FOR SAN ONOFRE UNITS 2 AND 3 SOUTHERN CALIFORNIA EDISON

DOCUMENT NO. 1370-ICE-1302, Rev. 01

Nuclear Power Systems
COMBUSTION ENGINEERING, INC.
Windsor, Connecticut

Prepared By R. F. Hoffman Date 11/2/84
R. F. Hoffman, Systems Interaction and Operation

Approved By C. A. Chambers Date 11/2/84
C. A. Chambers, Supervisor, Safety Status Monitoring Systems

Approved By T. M. Starr Date 11/2/84
T. M. Starr, Section Manager, Instrumentation Systems Design

Issue Date November 2, 1984

RECORD OF REVISIONS

NO.	DATE	PAGES INVOLVED	PREPARED BY	APPROVALS
00	9/27/84	All	R. F. Hoffman	K. R. Rohde T. M. Starr
01	11/2/84	19,21,40,56,75 76,78,84,95,99	R. F. Hoffman	C. A. Chambers T. M. Starr

ABSTRACT

NUREG-0737, Supplement 1, requires that a "written safety analysis" shall be prepared for the Safety Parameter Display System (SPDS). The safety analysis shall describe the basis on which the selected parameters are sufficient to assess the safety status of critical functions for a wide range of events.

The requirements for an SPDS have been met by San Onofre Units (SONGS) 2 and 3 by the Accident Monitoring System (AMS), designed and built by Combustion Engineering.

This document fulfills the requirement for a "written safety analysis" by describing:

1) basis for parameter selection for the SPDS

2) basis for algorithms used in the SPDS

3) how human factors were incorporated into AMS design

4) verification and validation of the AMS

5) compliance with NRC regulations

This is not a design document but is an assessment of the AMS design useful in licensing that system.

Table of Contents

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Abbrevation	Definition
A/C	Air Conditioning
AMS	Accident Monitoring System
AUX	Auxiliary
CCAS	Containment Cooling Actuation Signal
CCW	Component Cooling Water
CEA	Control Element Assembly
CEDM	Control Element Drive Mechanism
CFMS	Critical Function Monitoring System
CIAS	Containment Isolation Actuation Signal
CLR	Cooler
CNMT	Containment
CNTL	Control
COND	Condenser
CPIS	Containment Purge Isolation Signal
CRT	Cathode Ray Tube

List of Abbreviations (Continued)

Abbrevation	Definition
CSAS	Containment Spray Actuation Signal
DISCH	Discharge
FW	Feedwater
FWPT	Feedwater Pump Turbine
HDR	Header
HDSR	Historical Data Storage and Retrieval
HPSI	High Pressure Safety Injection
HX	Heat Exchanger
I/C	Inside Containment
ICC	Inadequate Core Cooling
INPO	Institute for Nuclear Power Operations
Inst. Air	Instrument Air
ISO	Isolation
LD	Letdown
LOCA	Loss of Coolant Accident

List of Abbreviations (Continued)

Abbrevation	Definition
LP	Loop
LPSI	Low Pressure Safety Injection
MON	Monitor
MSIS	Main Steam Isolation Signal
MSIV	Main Steam Isolation Valve
O/C	Outside Containment
PRESS	Pressure
PZR	Pressurizer
QSPDS	Qualified Safety Parameter Display System
Rad	Radiation
RC	Reactor Coolant
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
REGEN	Regenerative
SCE	Southern California Edison

List of Abbreviations (Continued)

Abbrevation	Definition
SDCS	Shutdown Cooling System
SG	Steam Generator
SI	Safety Injection
SIAS	Safety Injection Actuation Signal
SPDS	Safety Parameter Display System
SUCTN	Suction
TEMP	Temperature
TK	Tank
UVR	Under Voltage Relay
VOL	Volume
WTR	Water

I. SAFETY FUNCTIONS

A. DESCRIPTION OF SAFETY FUNCTIONS

Southern California Edison has installed an Accident Monitoring System (AMS) which comprises a Safety Parameter Display System (SPDS) known as the Critical Function Monitoring System (CFMS), seismically qualified Safety Parameter Display System (QSPDS) and an enhanced Historical Data Storage and Retrieval System (HDSR). The purpose of the AMS is to provide the control room personnel with concise, understandable, and integrated information to assist in assessing plant status during all modes of operation. The AMS also assists in assessing abnormal plant behavior following a reactor trip, including those events that lead to inadequate core cooling, which help prevent fuel damage and radiation releases to the public.

The SPDS utilizes the safety function concept. Safety functions introduce a systematic approach for mitigating the consequences of plant

transients and accidents. A critical safety function (as applied to a nuclear power plant) is defined as a group of actions that prevent core melt or minimize radiation releases to the general public. The actions may result from automatic or manual actuation of a system (e.g., reactor protection system generates a trip), passive system performance (e.g., safety injection tanks feed water to the reactor coolant system) or from natural feedback designed into the plant (control of reactivity by voiding in the reactor). Using safety functions, the operator observes the plant's state and determines if safety functions are jeopardized; and, if so, determines appropriate success paths and takes control actions along these success paths to ensure the safety functions are accomplished.

The safety functions grouped into the classes suggested in NUREGS-0696, 0835 and 0737, Supplement 1, are related to the CFMS. Although the titles of the critical functions differ between the NUREGS and their application in the CFMS, the definitions are the same. The correlation between the two follows:

NUREG-0696, 0835,0737 (Supplement 1)	CFMS
Reactivity Control	Core Reactivity Control
Reactor Core Cooling and Heat Removal From the Primary System	Core Heat Removal Control RCS Heat Removal Control
Reactor Coolant System Integrity	RCS Inventory Control RCS Pressure Control
Radioactivity Control	Radiation Emissions Control Containment Isolation Control
Containment Integrity	Containment Temperature/ Pressure Control

Descriptions of each of the critical functions follows:

The purpose of the first safety function, Reactivity Control, is to monitor those parameters that affect reactivity, and assist in maintaining the reactor shut down following reactor trip. Reactivity is controlled in the short term by insertion of the control rods and/or through the natural feedback mechanism in the reactor coolant. In the long term, reactivity is controlled by the addition of borated water to the reactor coolant system. Borated water can be added to the reactor coolant system using the charging and boric acid addition portions of the chemical and volume control system, the high and low pressure safety injection system and/or the safety injection tanks (reference 6).

The purpose of the second and third safety functions, Reactor Coolant System (RCS) pressure and RCS Inventory Control, is to monitor parameters that indicate that the core is covered with an effective coolant medium. RCS pressure control can involve either pressure maintenance or pressure limitation. Likewise, RCS

Inventory Control can invclve either inventory maintenance or inventory limitation. Under normal circumstances, RCS Pressure and inventory control are maintained automatically by the pressurizer pressure and level control systems. These systems use the pressurizer spray valves and the letdown system to limit pressure and inventory respectively, and they use the pressurizer heaters and charging system to maintain pressure and inventory respectively. If the pressure and level control systems are unable to limit RCS pressure and inventory, the pressure and inventory can be kept within bounds by action of the primary safety valves. In the event that RCS inventory and/or pressure becomes low due to an opening in the reactor coolant pressure boundary or excessive cooling of the reactor coolant system from excess steam flow, RCS inventory is maintained by injection of borated water by the safety injection system or the safety injection tanks (reference 6).

The purpose of fourth safety function, Core Heat Removal, is to monitor the ability to remove the heat generated in the core by radioactive decay following reactor trip and transfer it to a point where it can be removed from the RCS. This is accomplished by passing a coolant medium through the core to a heat removal point. Normally, the reactor coolant pumps are used to provide forced reactor coolant flow through the reactor core to the steam generators. In the absence of forced reactor coolant flow, the core can still be cooled by natural circulation induced by a temperature differential from the steam generators to the core. (This implies that the steam generators must be available to act as a heat sink). If natural circulation cannot be established, heat can be removed from the core by boiling and movement of the steam to a point such that it can be discharged through an opening in the reactor coolant system piping (reference 6).

The purpose of the fifth safety function, RCS Heat Removal, is to monitor the system's ability to transfer heat from the reactor coolant to another heat sink. RCS heat removal is normally accomplished by transferring heat from the reactor coolant to the secondary system in the steam generator. The secondary system water is supplied by the main feedwater system or the auxiliary feedwater system. Reactor coolant heat can be transferred to the component cooling water via the shutdown cooling heat exchanger, provided that the reactor coolant system pressure is less than the shutdown cooling system pressure interlock setpoint. If no other heat sink is available, reactor coolant system heat removal can also be accomplished by discharging the hot reactor coolant directly into the containment through a pressure boundary opening or a primary relief valve (reference 6).

The purpose of the sixth safety function, Containment Isolation, is to prevent release of radioactivity from the containment by ensuring that all normal containment penetrations are closed off when containment isolation is required.

Containment Isolation uses a system and component type logic measuring containment pressure, electronic equipment to generate and transmit an isolation signal when the containment pressure exceeds a setpoint, and a set of valves for isolating each containment penetration. (These valves are generally part of other systems also.) Each containment penetration is provided with two isolation valves, one inside containment and one outside containment (reference 6).

The purpose of the seventh safety function, Containment Temperature and Pressure Control, is to prevent overstress of the containment structure and damage to other equipment from a hostile environment by keeping containment pressure and temperatures within prescribed limits. Containment pressure and temperature are controlled using the containment spray system and the containment cooling system (reference 6).

The purpose of the eighth safety function, Radiation Emissions control, is to prevent radioactive releases. The critical function monitors releases from the primary coolant into containment by monitoring

containment radiation. This critical function assists in monitoring releases from various areas around the plant outside containment by monitoring the plant vent stack, the containment purge stack and condenser air ejector radiation (reference 6).

The first five safety functions have priority relative to the others as shown in Figure 1. In general, reactivity control is the foremost function because the amount of heat that must be removed from the core is determined by how well this function is accomplished. Next in precedence are those functions for appropriately maintaining a core cooling medium. To achieve this, actions must be accomplished to maintain an adequate reactor coolant system inventory and an appropriate reactor coolant system pressure. Finally, if core heat removal is not carried out, then coolant system heat removal is irrelevant (reference 6).

Figure 1: Hierarchy of first five safety functions

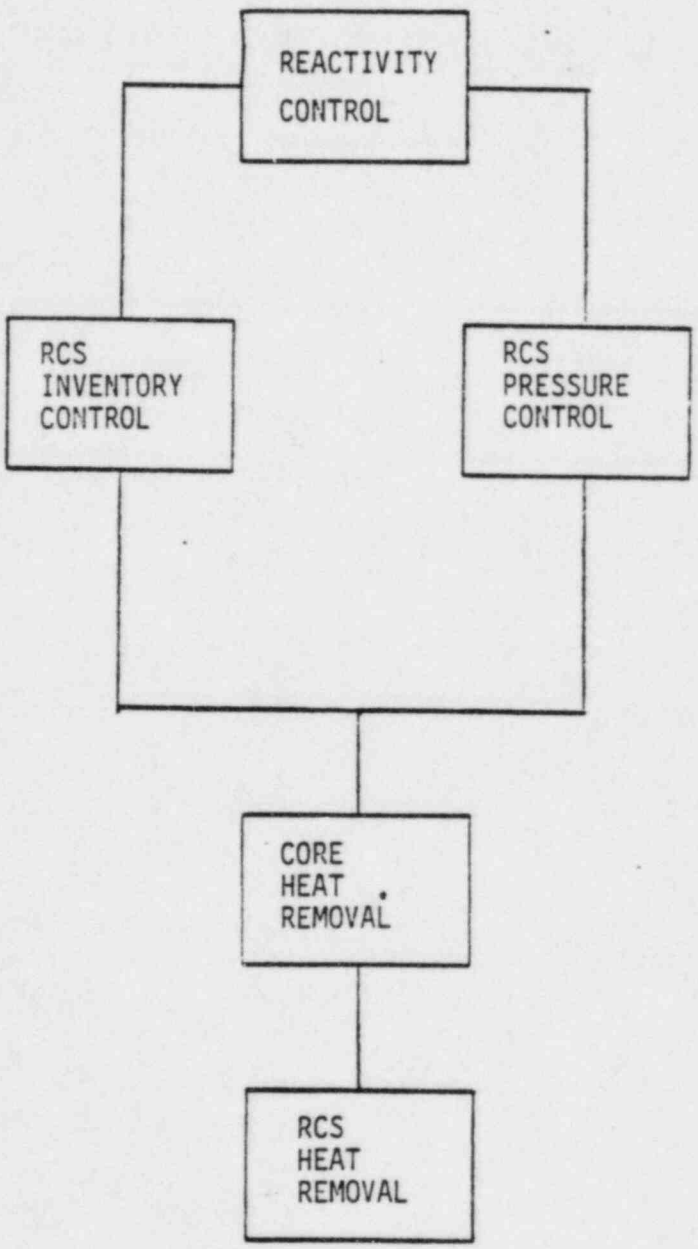


FIGURE 1

Advanced human engineering techniques have been incorporated into the design of the CFMS. One way this is accomplished is by displaying only pertinent information related to a safety function, and by designing displays so that they are easily understood by the operators.

The displays have been arranged in a hierarchy (Figure 3). The hierarchy consists of three levels:

1) Level 1 - Overall plant status

2) Level 2 - Function status

3) Level 3 - Subfunction diagnostic status

The Level 1 display provides the operator with a broad overview of the status of all the safety functions. Level 2 displays more information on a safety function at the system level (i.e.; primary system, secondary system, etc.) Level 3 displays provide even more detailed information on a sub-function level (i.e., Safety Injection System, Main Feedwater System, etc.)

When an abnormality occurs, the affected safety function on the Level 1 display is highlighted by a color change and on-off blinking. The operator is then guided in a systematic fashion to the Level 2 and 3 displays to obtain more information on the nature of the abnormality.

I.B.1 Basis for Parameter Selection

Supplement 1 to NUREG-0737 specifies that the SPDS must provide (as a minimum) plant operators with information about the following 5 areas: (The CFMS addresses these areas as eight unique critical safety functions which are noted in the parentheses):

1) Reactivity Control (same name)

2) Reactor Core Cooling and Heat Removal from the primary system (Core Heat Removal, RCS Heat Removal)

3) Reactor coolant system integrity (RCS Inventory Control, RCS Pressure Control)

4) Radioactivity control (Radiation Emissions Control, Containment Isolation)

5) Containment integrity (Containment Temperature/Pressure Control)

Additional guidance used to select SPDS parameters was obtained from Reg. Guide 1.97 and operating experience. Many of the parameters discussed below are monitored for a variety of reasons but will be discussed only with respect to their use in maintaining safety functions. The basis for the parameters selected to meet the requirements of the subject areas identified in Generic Letter P2-33 is as follows:

1) Reactivity Control

The purpose of the reactivity control critical function is to maintain control over the core nuclear process after a reactor trip has occurred and provide the operator with the status of conditions within the reactor core. The CFMS meets the objective by measuring various core parameters and conditions including

1) CEA rod bottom contacts
2) CEDM main power bus under voltage relays
3) Neutron flux

4) wide range log power

5) hot and cold leg temperatures

6) RCS boron concentration

The above parameters are monitored to alert the operator to possible loss of shutdown margin following a reactor trip.

The CFMS monitors and displays reactor power in all ranges and rate of change of power. This provides the means to monitor core flux conditions throughout all ranges of reactor operation. The CFMS monitors post trip power, reactivity addition, and reactor trip status. Based upon the above evaluation, these parameters are sufficient to provide the operator with indication of reactivity control for a range of plant conditions.

2) Reactor Core Cooling and Heat Removal from the Primary System

The objective of this area is to provide sufficient indication such that an operator can determine if the reactor core is being adequately cooled and heat is being sufficiently removed from this system.

a) Core Heat Removal

The purpose of the core heat removal critical function is to transfer heat generated in the reactor core to the primary coolant system, where heat will be transferred out of the RCS. A loss of core heat removal is indicated by the CFMS by high core exit temperatures, a loss of primary coolant subcooling, and/or voiding in the reactor vessel and the hot legs. In order to monitor this critical function, the following parameters are measured by the CFMS:

1) hot and cold leg temperatures - this enables monitoring adequate forced or natural circulation cooling or shutdown cooling system operation.

2) reactor vessel level - the reactor vessel level is measured from the top of the core to the top of the reactor vessel head. A low reactor vessel level indicates a potential for core uncovery.

3) Core exit temperature - thermocouples are located just above the core. Rising core exit temperature indicates increasing cladding temperature caused by core uncovery while falling core exit temperatures indicate decreasing cladding temperature. Core exit temperature is also used for calculating the saturation margin at the core exit, another indicator of the trend of cladding temperature in the core.

4) Reactor coolant pump load - this is used to monitor the formation of voids in the reactor coolant system. Decreasing pump load may indicate void formation.

b) RCS Heat Removal

The purpose of this critical function is to transfer the heat that is in the primary coolant to one of the following heat sinks: the steam generator, shutdown cooling system (SDCS), or containment (when there is an opening in the primary system). This algorithm will monitor core conditions following a reactor trip.

The essential parameters monitored by the CFMS are:

1) LPSI header flows, temperatures, SDCS valve positions - the status of these parameters are monitored during shutdown cooling operation to ensure adequate heat removal from the RCS.

2) Steam generator levels, feedwater flows - these are monitored to observe proper cooling of the RCS while the plant is in a mode other than shutdown cooling.

3) Charging flow, LPSI and HPSI flow - these flows are monitored to ensure adequate heat removal capability in the event that inventory remplacement is needed following SIAS.

The monitored parameters - core exit temperatures, cold leg temperatures, saturation margin, steam generator level, steam generator pressure, reactor vessel level, shutdown cooling temperatures and flow and the safety injection flow are sufficient for the operator to assess RCS Heat Removal and Core Heat Removal for a wide range of conditions.

3) Reactor Coolant System Integrity

The objective of this critical function is to provide sufficient indication such that an operator is able to determine that primary coolant system boundaries are maintained. The CFMS meets this objective by monitoring two critical Safety functions, RCS Inventory Control and RCS Pressure Control.

a) RCS Inventory Control

The objective of this critical function is to monitor the system's ability to keep the core covered with an effective coolant medium. Maintaining RCS inventory ensures maintaining adequate core cooling. The critical function algorithm considers only the initial loss of RCS inventory control. Continued inventory losses are monitored by the core heat

removal critical function (e.g., reactor vessel level). The parameters that are monitored by the CFMS as follows:

i) Pressurizer Level - excessively low pressurizer level could indicate a large RCS coolant contraction (from an excess cooldown event) or a loss of inventory (from a steam generator tube rupture or LOCA).

ii) Quench Tank Level, Temperature, Pressure - these parameters monitor discharge from the primary safety valves. A high level, temperature and pressure may indicate potential for relieving the Quench Tank contents into containment and indicate an abnormally large discharge of RCS inventory.

iii) Relief Valve Discharge Temperature - this is another indicator of primary safety valve discharge. A

continually high relief valve discharge temperature may indicate abnormally large discharge of RCS inventory.

b) RCS Pressure Control

This critical safety function monitors the system's ability to maintain an effective coolant medium by ensuring RCS pressure is within bounds. The parameters that are monitored by the CFMS are:

i) Pressurizer Pressure - this parameter is used to monitor the maintenance of subcooled margin in the reactor coolant. This is also used to monitor (in conjunction with cold leg temperature), the approach to material fracture limits. This is also used to monitor transients with a high rate of change of pressure, or high sustained pressurizer pressure.

ii) Cold Leg Temperature - this is used, along with pressurizer pressure, to ensure that over-pressurization of the primary system does not occur when the RCS is cold (thus avoiding violation of material fracture requirements).

The monitored parameters, pressurizer pressure, pressurizer level, quench tank temperature, cold leg temperature, quench tank level and quench tank pressure assess RCS integrity for a wide range of operating conditions.

4) Radioactivity Control

The objective of this critical function is to provide sufficient indication such that an operator can determine that radioactive substances are not being released to the environment in an uncontrolled manner. The CFMS meets this objective by monitoring two critical safety functions: Radiation Emissions Control & Containment Isolation.

a) Radiation emissions control - this critical function algorithm monitors potentially harmful radiation from the primary system to containment and from the plant into the environment. The essential parameters that are monitored are:

i) condenser air ejector radiation - this detects high Xenon and Krypton gas concentration which may indicate a steam generator tube rupture.

ii) vent stack radiation - this detects radiation leaving the plant by way of the ventilation system.

iii) containment radiation - this detects radioactive particulate concentrations in containment following a LOCA.

iv) containment dome radiation - this detects radioactive gas in the upper portion of the containment building following a LOCA.

v) Purge stack radiation - this detects radiation leaving the plant by way of the containment purge system.

b) Containment Isolation - the purpose of this critical function is to prevent release of radioactivity from containment by assuring that pipes that penetrate containment close upon receiving isolation signals. Isolation of these valves prevent release of radioactive water or steam from leaving containment and uncontrolled blowdown of the secondary side in the case of a steam line break. The valves monitored by the CFMS are found in Table 1, and are listed by classes below:

i) valves that close on containment isolation signal (CIAS). This prevents release of radioactivity outside containment following a primary or secondary break.

ii) valves that close on containment purge isolation signal (CPIS). This prevents release of radioactivity from the containment purge system to the environment.

iii) valves that close on Safety Injection Actuation (SIAS). This prevents release of radioactivity outside containment following a primary or secondary break.

iv) valves that close on Main Steam Isolation (MSIS). These valves prevent excessive blowdown of the secondary side following a steam line break.

The monitored parameters for radiation emissions control and containment isolation provide control room operators with sufficient indication of any potential uncontrolled radiation release.

5) Containment Integrity

The objective of this critical function is to provide sufficient indication such that an operator can determine if a containment boundary is being maintained to control radioactive releases.

a) Containment temperature/pressure control - the purpose of this critical function is to prevent potentially large radioactivity releases from containment by maintaining containment pressure within design limits. The following parameters are monitored by the CFMS:

i) containment fan cooler operability - containment fan coolers are used to reduce containment temperature and pressure. The CFMS will generate an alarm whenever more than two out of the four fan coolers are not working, when they are required to operate.

ii) containment spray flow - containment sprays are necessary to reduce containment pressure following a LOCA or Main Steam Line Break (MSLB) inside containment.

iii) containment pressure - this parameter is observed to monitor the effectiveness of the containment pressure mitigating systems.

iv) containment temperature - a persistently high containment temperature may adversely affect the operation of safety systems in containment. This parameter can also provide indication of gas combustion in containment.

I.B.2 Bases for Algorithms and Legs

The basis for all the CFMS algorithms is to alert the operator when control of a critical function could be lost. For example, if the shutdown cooling heat exchangers malfunction during shutdown cooling operation, control over RCS heat removal could be lost. An alarm is generated, therefore, to alert the operator. A description for all the alarm algorithms legs is given below for each critical function.

Reactivity Control

Core reactivity control monitors the status of various core parameters to assure controllability of the nuclear process, i.e., the function's objective is to maintain control over the core nuclear process after a reactor trip has been generated. Prior to a reactor trip, core, moderator and doppler feedbacks and boron concentration adjustments can compensate for small reactivity

changes. For larger reactivity changes and for a variety of plant malfunctions a reactor trip will automatically occur. After reactor trip, boron maintains the core in a shutdown condition. This critical function algorithm will therefore (1) ensure that a sufficient number of CEAs drop in on reactor trip and (2) there is sufficient boron in the core to maintain shutdown margin.

The following alarm legs monitor these conditions:

1) CEA Drop Malfunction - An alarm is generated if a sufficient number (more than 10) of CEAs have not dropped following a reactor trip.

2) High Post Trip Power - This algorithm leg detects abnormal post trip increases in neutron count rate indicative of a flux increase.

3) Thermal Reactivity Addition - This algorithm leg detects high source range count rates indicative of flux increases in the cold shutdown condition.

4) Low Boron Concentration - If an insufficient number of CEAs have dropped in following a reactor trip (as determined in the CEA Drop Malfunction leg) core reactivity can be controlled by having sufficient boron in the core. An alarm is generated if the algorithm determines there is not enough boron in the core to maintain shutdown margin.

Core Heat Removal

The purpose of the critical function is to monitor the system's ability to transfer heat from the reactor core to the primary coolant system. The primary mode of core heat removal is by forced circulation of coolant by the reactor coolant pumps (RCPs). If the

RCPs are unavailable, natural circulation of coolant will remove heat from the core. In the case where there is a break in the primary system, steam produced by water boiling in the core will remove heat.

If sufficient inventory is lost from the primary system during a LOCA, the fuel cladding may heat up and rupture, releasing radioactivity into the primary system. The core heat removal critical function will alert the operator to the approach to inadequate core cooling conditions using the following algorithm legs.

1) Low reactor coolant pump load - One of the early indicators of a LOCA is the decrease in RCP load due to voiding. An alarm is generated whenever RCP load falls below a setpoint.

2) Low reactor vessel level - An alarm is generated when level in the reactor vessel has decreased to the bottom of the hot leg. This will alert the operator to the potential for core uncovery.

3) Core saturation margin - This leg alerts the operator to the transition from subcooled to saturated fluid at the core exit.

4) Hi core ΔT (T_{hot} - T_{cold}) - This indicates lower circulation of primary fluid through the core than that needed to remove decay heat during natural circulation.

5) Hi core exit temperature - This indicates high cladding temperatures in the core as a result of core uncovery.

RCS Heat Removal

The objective of the RCS heat removal algorithm is to transfer heat generated and stored in the RCS to a heat sink. The critical safety function monitors the various means of heat removal to determine if heat is being removed from the RCS. While the RCS is intact, heat

is removed either from the steam generators or the shutdown cooling system. If there is a small break LOCA heat is removed by a combination of steam exiting the RCS through a break and steam generator cooling. For a large break LOCA, heat is removed almost exclusively through the break.

The alarm algorithm legs are therefore:

1) Steam Generator Not Cooling

An alarm is generated to alert the operator that steam generator heat removal capability is lost based on low feedwater flows and steam generator levels. This alarm will occur if the reactor has tripped, the shutdown cooling system is not aligned and the RCS is still subcooled.

2) Shutdown Cooling System Not Cooling

An alarm is generated to indicate inadequate shutdown cooling operation while the system is in cold shutdown. The alarm is based on Low Pressure Safety Injection (LPSI) flow and LPSI header temperature.

3) Low Safety Injection/Feedwater Cooling

An alarm is generated if the combined cooling capability of the steam generators and safety injection systems are insufficient to remove decay heat during a small break LOCA. The algorithm monitors feedwater and safety injection flows, RCS saturation margin, and RCS heatup rate.

4,5) Low Safety Injection System Pump Flow, Emergency Core Cooling System Not Cooling

Both of these algorithm legs generate alarms whenever the ECCS system is delivering .nadequate safety injection flow to the RCS. This alarm is useful in monitoring large and small break LOCAs. The algorithms monitor safety injection flow vs. pressurizer pressure performance, and safety injection flow vs time following a large break (before and after RAS).

Reactor Coolant System (RCS) Inventory Control

The objective of this critical safety function is to keep the core covered with an effective coolant medium. The critical function compares the group of actions to maintain control over coolant volume or mass. Normally, inventory is maintained by the Pressurizer Level Control System (PLCS). Normal control over inventory is lost if level cannot be maintained in the

pressurizer. The algorithm therefore monitors the initial loss of inventory control (further losses are monitored by the RCS and core heat removal critical functions). The opening of the primary relief valves relieves inventory to the Quench Tank when the RCS is over-pressurized. Excessive blowdown through the relief valves though can jeopardize RCS inventory control and is therefore monitored. The alarm algorithm legs are therefore:

1) Low Pressurizer Level - Abnormal fluid contractions (such as an excess cooldown) or excess inventory losses (such as a LOCA) may cause pressurizer level to significantly decrease. An alarm is therefore provided.

2) Quench Tank Level, Pressure, Temperature - Primary relief valve discharges are monitored by the CFMS. High Quench Tank level, pressure or temperature indicates abnormally

large relief valve discharge, threatening inventory control. All three parameters are monitored since they may increase at an unequal rate.

3) Relief Valve Discharge Temperature - An alarm occurs whenever the relief valves open. If the alarm remains on below the relief valves blowdown pressure, inventory control is threatened.

RCS Pressure Control

This critical function, along with RCS Inventory Control, monitors the plant's ability to maintain an effective coolant medium around the core. The objective of this critical function algorithm is to maintain pressure between the high pressurizer pressure trip setpoint and the minimum pressure needed to maintain 20°F

subcooling. Alarms are generated when RCS pressure or the rate of change of pressure is expected to exceed these bounds. The algorithm legs are therefore:

1) High pressurizer pressure/rate - An alarm is generated whenever the rate of change is expected to exceed the bounds listed above, or whenever there is a high sustained pressurizer pressure.

2) Low Subcooled Margin - An alarm is generated if subcooled margin goes below a setpoint indicating an approach to inadequate core cooling condition.

3) Cold Stress Temperature - In addition to the above alarms, an alarm is generated to detect overpressurization of the primary system while in a cold condition, to prevent violation of material fracture requirements.

Radiation Emissions Control

The objective of this critical safety function is to monitor releases of radiation from the primary coolant system to containment, and from the plant as a whole to the environment. The algorithm legs are therefore:

1) High Containment Radiation - An alarm is generated whenever a high particulate concentration occurs in containment, indicating a LOCA.

2) High Containment Dome Radiation - An alarm is generated whenever a high radioactive gas concentration occurs in the containment dome, indicating a LOCA with fuel cladding failure.

3) High Condenser Air Ejector Radiation - An alarm is generated whenever a high xenon and krypton gas concentration occurs at the condenser air ejector, indicating a steam generator tube rupture.

4) High Vent/Stack - An alarm is generated whenever radiation is detected leaving the plant through the continuous vent stack. This will detect releases that occur from a number of sources throughout the plant (waste tanks, vents, etc.)

5) Hi Purge Stack - An alarm is generated whenever radiation is detected leaving the plant through the purge stack. This will detect releases that occur from the containment purge system.

Containment Isolation

The purpose of the containment isolation critical function is to prevent radioactivity releases from containment by assuring that

valves in piping penetrating containment close on demand. There are a number of signals that will close containment penetration isolation values. This algorithm monitors the closure of isolation valves actuated from the following signals:

1) Containment Isolation Actuation Signal (CIAS) - This signal isolates a number of containment penetrations based on either a low pressurizer pressure or high containment pressure signal indicative of a steam line break or LOCA.

2) Containment Purge Isolation Signal (CPIS) - This signal occurs on a high radiation sensed in containment.

3) Safety Injection Actuation Signal (SIAS) - This signal isolates containment penetrations based on a low pressurizer pressure or high containment pressure. This prevents release of radioactive water outside containment following a LOCA.

4) Main Steam Isolation Signal (MSIS) - This signal occurs to prevent uncontrolled blowdown of the secondary side following a Steam or Feedwater Line Break.

Containment Temperature/Pressure Control

The objective of this critical function is to prevent overstress of the containment or damage to vital equipment by keeping temperature and pressure within prescribed limits. During a LOCA or steam line break inside containment, temperature and pressure increase. At +4 psig containment pressure, a Containment Cooling Actuation Signal (CCAS) occurs, actuating containment fan coolers. At +12 psig a Containment Spray Actuation Signal (CSAS) occurs actuating containment sprays. Proper operation of these two systems should prevent approach to containment design limits. This algorithm therefore monitors the operation of the pressure mitigating systems.

The algorithm logs are therefore:

1) Fan Coolers - After CCAS initiation, if less than 2 fan coolers are operating an alarm will be generated.

2) Low Spray Flow - After CSAS, if there is insufficient spray flow to containment, an alarm will be generated.

3,4) Containment Pressure Change and High Containment Pressure - These two algorithm legs monitor the effectiveness of the above containment pressure mitigating systems. An alarm is generated if the magnitude or rate of change of pressure exceed limits.

5) Low Containment Pressure - An alarm occurs if containment pressure decreases below atmospheric pressure as a result of excessive spray flow.

6) High Containment Temperatures - An alarm is generated if containment temperatures are high. This is to alert the operator of 1) possible adverse effect on safety equipment, or 2) the possibility of gas combustion taking place in containment.

I.B.3 Correlation of SPDS Parameters to the Five Critical Functions of Supplement 1, NUREG 0737.

The five critical functions defined in NUREG-0696, 0835, and 0737 supplement 1 are:

1) Reactivity control
2) Reactor core cooling and heat removal from the primary system
3) Reactor coolant system integrity
4) Radioactivity control
5) Containment integrity

The critical functions within the CFMS are:

1) Reactivity Control
2) Reactor Coolant System (RCS) Inventory Control
3) RCS Pressure Control
4) Core Heat Removal Control

5) RCS Heat Removal Control

6) Containment Pressure/Temperature Control

7) Containment Isolation

8) Radiation Emissions Control

The critical functions defined in NUREGS-0696 and 0737·Supplement 1 correspond to the critical functions applied to the CFMS as shown below:

NUREG-0696,0737(Sup.1)	CFMS
1. Reactivity control	Core Reactivity control
2. Reactor core cooling and heat removal from the primary system	Core Heat Removal RCS Heat Removal
3. Reactor coolant system integrity	RCS Inventory Control RCS Pressure Control

NUREG-0696,0737(Sup.1)	CFMS
4. Radioactivity control	Radiation Emissions Control
	Containment Isolation
5. Containment Integrity	Containment Temperature/
	Pressure Control

Table 1 identifies the specific parameters monitored for each of the safety functions.

TABLE 1

SONGS Unit 2 and 3

Safety Parameter Display System (SPDS)

Parameter Selection

	POINT ID	ENGLISH DESCP.	RANGE
I	Core Reactivity Control		
	Y1091	CEDM Main power bus uvr 1	On/Off
	Y1092	CEDM Main power bus uvr 2	On/Off
	Y1093	CEDM Main power bus uvr 3	On/Off
	Y1094	CEDM Main power bus uvr 4	On/Off
	Y1542 to	CEA 01 Bottom contact to	On/Off
ooo	Y1632	ooo CEA 91 Bottom contact	On/Off
	XJ005	Neutron flux startup Ch. 1	$1x10^{0}$ - $1x10^{5}$ cnts/s
	XJ002C	High log pwr lvl Ch. 3	$2x10^{-8}$ to $2x10^{2}$ pct.
	T111X	Hot leg temp Loop 1	525-625°F
	T121X	Hot leg temp Loop 2	525-625°F
	T111XA	Hot leg SGE089 Temp Ch. A	0-710°F
	T121XB	Hot leg SGE088 Temp Ch. B	0-170°F
	T111Y	Cold leg temp loop 1A	525-625°F
	T125	Cold leg temp loop 2A	0-600°F
	T115	Cold leg temp loop 1B	0-600°F
	T121Y	Cold leg temp loop 2B	525-625°F
	T111YA	Cold leg LP 1A temp Ch. A	0-710°F
	T125A	Cold leg LP 2A temp Ch. A	0-710°F
	T115B	Cold leg LP 1B temp Ch. B	0-710°F
	T121YB	Cold leg LP 2B temp Ch. B	0-710°F
	A203	Boronometer	0-5000/ppm

POINT ID	ENGLISH DESCP.	RANGE
II Core Heat Removal		
T111X	Hot leg temp loop 1	525-625°F
T121X	Hot leg temp loop 2	525-625°F
T111XA	Hot leg SGE089 temp Ch. A	0-710°F
T121XB	Hot leg SGE088 temp Ch. B	0-710°F
T111Y	Cold leg temp loop 1A	525-625°F
T121Y	Cold leg temp loop 2B	525-625°F
T111YA	Cold leg LP 1A temp Ch. A	0-710°F
T115B	Cold leg LP 1B temp Ch. B	0-710°F
T125A	Cold leg LP 2A temp Ch. A	0-710°F
T121YB	Cold leg LP 2B temp Ch. B	0-710°F
T115	Cold leg temp Loop 1B	0-600°F
T125	Cold leg temp Loop 2A	0-600°F
KRVLPLN	Reactor Vessel Level (Plenum)	0 - 100° Pct.
KCET	Representative core exit temp	32 - 2300°F
KCTSM	CET temp sat margin	-2100-700°F
YI9160A	RCP 1A amps	0.0-1000 Amp
YS9161A	RCP 1B status	On/Off
YI9161A	RCP 2A amps	0.0-1000 Amp
YS9162A	RCP 2A status	On/Off
YI9163A	RCP 2B amps	0.0-1000 Amp
YS9163A	RCP 2B status	On/Off
YS9160A	RCP 1A status	On/Off
YI9161A	RCP 1B amps	0.0-1000 Amp

PLANT FUNCTION	DESCRIPTION	RANGE
III. RCS HEAT REMOVAL		
T351Y	LPSI HDR Temp	0-400°F
LT1114	SGE088 Level	0-100%
LT1115	SGE089 Level	0-100%
FT4725	Aux Fw Flowrate to SGE089	0.0-800.0 GPM
FT1111	Fw Flowrate to SGE089	0.0-1.602 $x10^4$ GPM
T111X	Hot Leg Temp Loop 1	525-625°F
T111Y	Cold Leg Temp Loop 1A	525-625°F
T115	Cold Leg Temp Loop 1B	0-600°F
T111XA	Hot Leg Temp SGE089 Ch. A	0-710°F
T111YA	Cold Leg Temp LP 1A Ch. A	0-710°F
T115B	Cold Leg Temp LP 1B Ch. B	0-710°F
LT1124	SGE089 Level	0-100%
LT1125	SGE088 Level	0-100%
FT4720	Aux Fw Flowrate SGE088	0.0-800.0 GPM
FT1121	FW Flowrate to SGE088	0.0-1.602x10^4 GPM
T121X	Hot Leg Temp Loop 2	525-625°F
T125	Cold Leg Temp Loop 2A	0-600°F
T121Y	Cold Leg Temp Loop 2B	525-625°F
T121XB	Hot Leg Temp SGE088 Ch. B	0-710°F
T125A	Cold Leg Temp LP2A Ch. A	0-710°F
T121YB	Cold Leg Temp LP2B Ch. B	0-710°F
ZL93371	SDC ISO VIV	Open/Closed
ZL93392	SDC ISO VIV	Open/Closed
ZL93773	SDC ISO VIV	Open/Closed

PLANT FUNCTION	DESCRIPTION	RANGE
III. RCS HEAT REMOVAL (Continued)		
Z93784	SDC ISO VIV	Open/Closed
ZL93362	SDC ISO VIV	Open/Closed
ZL93791	SDC ISO VIV	Open/Closed
T111X	Hot Leg Temp Loop 1	525-625°F
T111XA	Hot Leg Temp SGE089 Ch. A	0-710°F
P100X	Pzr. Pressure	1500-2500 PSIA
P102A	Pzr. Pressure	0-3000 PSIA
P100Y	Pzr. Pressure	0-3000 PSIA
T121X	Hot Leg Temp Loop 2	525-625°F
T121XB	Hot Leg Temp SGE088 Ch. B	0-710°F
XSIASA	SIAS Status 1	Normal/Actuated
XSIASB	SIAS Status 2	Normal/Actuated
YS92281	Charging Pump #1 Status	On/Off
YS9229	Charging Pump #2 Status	On/Off
YS92302	Charging Pump #3 Status	On/Off
F311	HPSI Cold Leg 1A Flowrate	0-500 GPM
F321	HPSI Cold Leg 1B Flowrate	0-500 GPM
F331	HPSI Cold Leg 2A Flowrate	0-500 GPM
F341	HPSI Cold Leg 2B Flowrate	0-500 GPM
F391	HPSI Hot Leg 1 Flowrate	0-500 GPM
F390	HPSI Hot Leg 2 Flowrate	0-500 GPM
F306	LPSI Header Flowrate	0-10000 GPM
Y1091	CEDM Main Power Bus Uvr 1	On/Off
Y1092	CEDM Main Power Bus Uvr 2	On/Off
Y1093	CEDM Main Power Bus Uvr 3	On/Off
Y1094	CEDM Main Power Bus Uvr 4	On/Off

POINT ID	ENGLISH DESCP.	RANGE
IV. RCS Inventory Control		
L110X	Pzr. Lvl Ch. X	0-100%
L110Y	Pzr. Lvl Ch. Y	0-100%
L116	Quench Tank Level	0-100%
P116	Quench Tank Pressure	0-25 PSIG
T116	Quench Tank Temperature	0-300°F
T107	Pzr Relief Valve RC2000 Discharge Temp	0-300°F
T108	Pzr Relief Valve RC201 Discharge Temp	0-300°F

PLANT FUNCTION	DESCRIPTION	RANGE
V. RCS Pressure		
T115	Cold Leg Temp. Loop 1B	0-600°F
T125	Cold Leg Temp. Loop 2A	0-600°F
T111YA	Cold Leg Temp. LP 1A Ch. A	0-710°F
T1158	Cold Leg Temp. LP 1B Ch. B	0-710°F
T125A	Cold Leg Temp. LP 2A Ch. A	0-710°F
T121YB	Cold Leg Temp. LP 2B Ch. B	0-710°F
P102A	Pzr. Pressure Ch. A	0-3000 PSIA
P102B	Pzr. Pressure Ch. B	0-3000 PSIA
P100X	Pzr. Pressure	1500-2500 PSIA
P100Y	Pzr. Pressure	1500-2500 PSIA
T101	Pzr. Water Temp	0-700°F
T111X	Hot Leg Temp Loop 1	525-625°F
T121X	Hot Leg Temp Loop 2	525-625°F
T111XA	Hot Leg SGE089 Temp. Ch. A	0-710°F
T121XB	Hot Leg SGE088 Temp. Ch. B	0-710°F

PLANT FUNCTION	DESCRIPTION	RANGE
VI. Radiation Emmissions		
1) Hi Cond. Air Eject		
RT78518	Cond. air eject rad mon	$1-1 \times 10^{6}$ mr/hr
2) Hi Vent/Stack		
RT7808A	Plant vent stack mon	$10 - 10^{7}$ mr/hr
3) Hi Cnmt		
RT7804C	Cnmt. airborne rad mon	$10 - 10^{7}$ cpm
4) Hi cnmt Dome		
RT7857	Cnmt. dome rad mon	$10^{-1} - 10^{5}$ mr/hr
5) Hi Purge Stack		
RT7828A RT7828B RT7828C	Purge Stack Radiation Monitor	$10^{-1} - 10^{-9}$ uCi/cc

PLANT FUNCTION	DESCRIPTION	RANGE
VII. Cnmt Isolation		
XC1ASA	CIAS Status 1	Normal/Actuated
XC1ASB	CIAS Status 2	Normal/Actuated
ZL05102	Pzr Stm Sample Iso Vlv	Closed/Open
ZL05111	Pzr Stm Sample Iso Vlv	Closed/Open
ZL92672	Letdown Iso Vlv	Closed/Open
ZL92051	Letdown Iso Vlv	Closed/Open
ZL05082	Hot Leg 1 Sample Iso Vlv	Closed/Open
ZL05172	Hot Leg 2 Sample Iso Vlv	Closed/Open
ZL05091	Hot leg I/C Iso Vlv	Closed/Open
ZL93341	SI Drain/Test Vlv	Closed/Open
ZL92172	RCP Bleedoff Osp Vlv	Closed/Open
ZL92181	RCP Bleedoff Iso Vlv	Closed/Open
ZL79112	Serv Wtr To Cnmt Sump Iso Vlv	Closed/Open
ZL05122	Pzr Surge Line Sample Iso Vlv	Closed/Open
ZL05131	Pzr Surge Line Sample Iso Vlv	Closed/Open
ZL58031	Cnmt Sump Pump Iso Vlv	Closed/Open
ZL58042	Cnmt Sump Pump Iso Vlv	Closed/Open
ZL5686	Fire Protection Iso Vlv	Closed/Open
ZL78052	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78101	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL98242	Cnmt Minipurge Outlet Vlv	Closed/Open
ZL99502	Cnmt Lg Vol. Purge Disch Vlv	Closed/Open
ZL98251	Cnmt Minipurge Outlet Vlv	Closed/Open
ZL99511	Cnmt Lg Vol Purge Disch Vlv	Closed/Open
ZL53881	Inst Air Supply Iso Vlv	Closed/Open
ZL54372	N2 Supply to Aux Sys Iso Vlv	Closed/Open

PLANT FUNCTION	DESCRIPTION	RANGE
VII. Cnmt Isolation (Continued)		
ZL75121	RC Drain Tank Pump Disch Iso Vlv	Closed/Open
ZL75132	RC Drain Tank Pump Disch Iso Vlv	Closed/Open
ZL78062	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78111	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78021	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78032	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78011	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL78002	Cnmt Air Rad Mon Iso Vlv	Closed/Open
ZL05161	RC Drain Tank Sample Iso Vlv	Closed/Open
ZL0514	RC Drain Tank Sample Iso Vlv	Closed/Open
ZL05152	Quench & RC Drn Tnk Smpl Iso Vlv	Closed/Open
ZL82042	MSIV (SGE089)	Closed/Open
ZL4051	Main Fw Stop Vlv SGE089	Closed/Open
ZT1105	Main Fw Bypass SGE089	0-100%
ZL40522	Fw Iso Vlv SGE089	Closed/Open
ZL62112	CCW Inlet Vlv	Closed/Open
ZL62162	CCW Outlet Vlv	Closed/Open
ZL99002	Cnmt. Norm A/C Inlet Vlv	Closed/Open
ZL99201	Cnmt. Norm. A/C Inlet Vlv	Closed/Open
ZL99712	Cnmt. Norm. A/C Outlet Vlv	Closed/Open
ZL99211	Cnmt. Norm. A/C Inlet Vlv	Closed/Open
ZL72582	Cnmt. Waste Gas Vent Hdr. Iso. Vlv	Closed/Open
ZL72591	Cnmt. Waste Gas Vent Hdr. Iso.Vlv	Closed/Open
ZL5434	N2 supply to SI tanks Iso. Vlv	Closed/Open
ZL82051	MSIV (SGE088)	Closed/Open
ZL40481	Fw Iso Vlv SGE088	Closed/Open
ZL4047	Main Fw Stop Vlv SGE088	Closed/Open
ZT1106	Main Fw Bypass SGE088 Vlv	0-100%

PLANT FUNCTION	DESCRIPTION	RANGE
VII. Cnmt Isolation (Continued)		
ZL98231	Cnmt Minipurge inlet Vlv	Closed/Open
ZL99491	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL98212	Cnmt minipurge inlet Vlv	Closed/Open
ZL99482	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL92042	Ld to regen hx control Vlv	Closed/Open
ZL02211	Ld to regen hx control Vlv	Closed/Open
ZL6212	CCW disch to non-crit loop	Closed/Open
ZL6213	CCW disch to non-crit loop	Closed/Open
ZL6218	CCW suctn from non-crit loop	Closed/Open
ZL6219	CCW suctn from non-crit loop	Closed/Open
ZL6223	CCW inlet Vlv	Closed/Open
ZL6236	CCW outlet Vlv	Closed/Open

PLANT FUNCTION	DESCRIPTION	RANGE
Containment Isolation-Main Steam Isolation Leg		
XMSISA	MSIS Status 1	Normal/Actuated
XMSISB	MSIS Status 2	Normal/Actuated
ZL40481	FW Iso Vlv SGE088	Closed/Open
ZL40522	FW Iso Vlv SGE089	Closed/Open
KXEFAS1	EFAS Status 1	Normal/Actuated
ZL40532	Blowdown Iso Vlv SGE089	Closed/Open
KXEFAS2	EFAS Status 2	Normal/Actuated
ZL40541	Blowdown Iso Vlv SGE088	Closed/Open
ZL40572	Blowdown Sample Line SGE089	Closed/Open
ZL40581	Blowdown Sample Line SGE088	Closed/Open
ZL47152	Aux. Fw Iso Vlv SGE089	Closed/Open
ZL82002	Main Stm Aux Fwpt SGE089	Closed/Open
ZL82011	Main Stm Aux Fwpt SGE088	Closed/Open
ZL82022	MSIV Bypass Vlv SGE089	Closed/Open
ZL82031	MSIV Bypass Vlv SGE089	Closed/Open
ZL82042	MSIV (SGE089)	Closed/Open
ZL82051	MSIV (SGE088)	Closed/Open
ZL82481	MSIV Bypass to Cond. SGE088	Closed/Open
ZL82492	MSIV Bypass to Cond. SGE089	Closed/Open
ZL84191	Atmos. Dump Vlv SGE088	Closed/Open
ZL84212	Atmos. Dump Vlv SGE089	Closed/Open
ZL47301	Aux. Fw Iso Vlv SGE088	Closed/Open
ZL47311	Aux. Fw Iso Vlv SGE089	Closed/Open
ZL47051	Aux. Fw. Cntl Vlv SGE088	Closed/Open
ZL47062	Aux. Fw. Cntl Vlv SGE089	Closed/Open
ZL4713	Aux. Fw. Cntl Vlv SGE089	Closed/Open
ZL47122	Aux. Fw. Cntl Vlv SGE088	Closed/Open

PLANT FUNCTION	DESCRIPTION	RANGE
Containment Isolation-Containment Purge Isolation Leg		
ZL99482	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL99491	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL99502	Cnmt lg vol purge disch Vlv	Closed/Open
ZL99511	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL9821	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL9823	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL98242	Cnmt minipurge outlet Vlv	Closed/Open
ZL98251	Cnmt minipurge outlet Vlv	Closed/Open
ZL98251	Cnmt minipurge outlet Vlv	Closed/Open
XCPISA	CPIS Status 1	Normal/Actuated
XCPISB	CPIS Status 2	Normal/Actuated

PLANT FUNCTION	DESCRIPTION	RANGE
Containment Isolation-Safety Injection Isolation Leg		
ZL05102	Pzr Steam Sample Iso Vlv	Closed/Open
ZL05111	Pzr Steam Sample Iso Vlv	Closed/Open
ZL92672	Letdown Iso Vlv	Closed/Open
ZL92051	Letdown Iso Vlv	Closed/Open
ZL05082	Hot Leg 1 Sample Iso Vlv	Closed/Open
ZL05172	Hot Leg 2 Sample Iso Vlv	Closed/Open
ZL05091	Hot Leg I/C Iso Vlv	Closed/Open
ZL93341	SI Drain/Test Vlv	Closed/Open
ZL92172	RCP Bleedoff Iso Vlv	Closed/Open
ZL92181	RCP Bleedoff Iso Vlv	Closed/Open
ZL79112	Serv wtr to cnmt sump iso Vlv	Closed/Open
ZL05122	Pzr surge line sample is Vlv	Closed/Open
ZL05131	Pzr surge line sample is Vlv	Closed/Open
ZL58031	Cnmt sump pump I/C iso Vlv	Closed/Open
ZL58042	Cnmt sump pump O/C iso Vlv	Closed/Open
ZL5686	Fire protection iso Vlv	Closed/Open
ZL78052	Cnmt air rad mon iso Vlv	Closed/Open
ZL78101	Cnmt air rad mon iso Vlv	Closed/Open
ZL98242	Cnmt minipurge outlet Vlv	Closed/Open
ZL99502	Cnmt lg vol purge disch Vlv	Closed/Open
ZL98251	Cnmt minipurge outlet Vlv	Closed/Open
ZL99511	Cnmt lg vol purge disch Vlv	Closed/Open
ZL53881	Inst air supply iso Vlv	Closed/Open
ZL54372	N2 supply to aux sys iso Vlv	Closed/Open
ZL75121	RC drain tank pump disch iso Vlv	Closed/Open
ZL75132	RC drain tank pump disch iso Vlv	Closed/Open
ZL78062	Cnmt air rad mon iso Vlv	Closed/Open
ZL78111	Cnmt air rad mon iso Vlv	Closed/Open

PLANT FUNCTION	DESCRIPTION	RANGE
Containment Isolation-Safety Injection Isolation Leg (Continued)		
ZL78021	Cnmt air rad mon iso Vlv	Closed/Open
ZL78032	Cnmt air rad mon iso Vlv	Closed/Open
ZL78011	Cnmt air rad mon iso Vlv	Closed/Open
ZL78002	Cnmt air rad mon iso Vlv	Closed/Open
ZL05161	RC drain rank sample iso Vlv	Closed/Open
ZL05141	Quench tank sample iso Vlv	Closed/Open
ZL05152	Quench & RC drn tk smpl iso Vlv	Closed/Open
ZL4051	Main Fw stop Vlv SGE089	Closed/Open
ZT1105	Main Fw bypass Vlv SGE089	0-100%
ZL40522	Fw iso V/V SGE089 Vlv	0-100%
ZL99002	Cnmt norm A/C inlet Vlv	0-100%
ZL99201	Cnmt norm A/C inlet Vlv	0-100%
ZL99712	Cnmt norm A/C outlet Vlv	0-100%
ZL99211	Cnmt norm A/C outlet Vlv	0-100%
ZL72582	Cnmt waste gas vent hdr iso Vlv	Closed/Open
ZL72591	Cnmt waste gas vent hdr iso Vlv	Closed/Open
ZL5434	N2 supply to S1 tanks iso Vlv	Closed/Open
ZL40481	Fw iso Vlv SGE088	Closed/Open
ZL4047	Main fw stop Vlv SGE088	Closed/Open
ZT1106	Main fw bypass SGE088 Vlv	0-100%
ZL98231	Cnmt minipurge inlet Vlv	Closed/Open
ZL99491	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL98212	Cnmt minipurge inlet Vlv	Closed/Open
ZL99482	Cnmt lg vol purge inlet Vlv	Closed/Open
ZL92042	Ld to regen hx control Vlv	Closed/Open
ZL02211	Ld to regen hx control Vlv	Closed/Open
XSIASA	SIAS status 1	Normal/Actuated
XSIASB	SIAS status 2	Normal/Actuated

PLANT FUNCTION	DESCRIPTION	RANGE
VIII. Cnmt Temp/Press Control		
XCCASA	CCAS Status 1	Normal/Actuated
XCCASB	CCAS Status 2	Normal/Actuated
YS99531	Cnmt. Fan clr E399 Status	On/Off
YS99471	Cnmt. Fan clr E401 Status	On/Off
YS99392	Cnmt. Fan clr E400 Status	On/Off
YS99552	Cnmt. Fan clr E402 Status	On/Off
XCSASA	CSAS Status 1	Normal/Actuated
XCSASB	CSAS Status 2	Normal/Actuated
F338	Cnmt. Spray No. 1 Flowrate	0-3500/GPM
F348	Cnmt. Spray No. 2 Flowrate	0-3500/GPM
P351A	Cnmt. press	-4-20/PSIG
P352A	Cnmt. press	-4-85/PSIG
TT99112	Cnmt. dome temp	0-400°F

II. HUMAN FACTORS CONSIDERATIONS

The fundamental SPDS design objective is to serve as an operator aid to monitor the overall safety status of the plant. Human factors considerations were included in the SPDS design and implementation process.

The central focus of human factors relates to the consideration of human beings in the design of the man-made facilities that people use. The objectives of human factors in the design of these man-made facilities are:

1) to enhance functional effectiveness

2) to maintain or enhance certain human values in the process.

3) to enhance the machine's usability and practicability in stressful situations

4) to facilitate the man machine interface

The central approach of human factors is the application of relevant information about human characteristics and behavior to the design of man-made facilities that people use.

When designing the CFMS, the role of the SPDS user was taken in to consideration, the context of use (control room), and the design constraints impacting the human factors development.

It is appropriate to consider the SPDS in the context of a structured crew model, i.e., task analysis. The shift supervisor is designated as the primary SPDS user. The SPDS is intended to aid the Shift Supervisor in allocating resources and directing the crew during highly unusual, complex situations where problem detection and problem solving on a plant-wide scale is demanded. This is consistent with the goal-controlled, knowledge-based behavior articulated by Rasmussen's model. (Ref. 1)

The role of the human factors verification process assured that good design practices were used to engineer SCE's CFMS in direct support of these job related tasks.

One of the human factors design constraints is a direct consequence of the control room setting as it relates to viewing. Human factors design reflects a compromise between human factors, hardware/software limitations, and styles of use.

A preliminary SPDS evaluation by Yankee Atomic Electric Company for their power plant in Rowe, Mass. (Reference 2) yielded the following human factors requirements on the display format:

- Higher display update frequency
- Faster display page call-ups (< 5 seconds)
- Need for a top level display
- Provide parameter alarm capability
- Cues required for pages not displayed
- Should support normal operation

- Display some additional parameters

- Integrate with emergency procedures.

1) Higher display update frequency -

The CFMS displays are updated every 1 second. This is sufficient to keep the operator informed during a rapidly changing transient, but is also slow enough to keep the display from being confusing during a transient.

2) Faster display page call ups -

It takes no more than 5 seconds to call up a new display page. This will help keep the operator sufficiently up to date during a transient situation.

3) Need for a top level display

The CFMS has a top level display page which lists all the critical functions and their associated alarm legs. The operator can at any time return to the top level display page to gain an overall view of the plant safety status.

4) Provide parameter alarm capability

The CFMS provides visual alarms for parameters that exceed alarm setpoints which alert the operator to a change in parameter status.

5) Cues required for pages not displayed

A new alarm is indicated on every display page. This cues the operator to return to the top level page to obtain more information on the nature of the alarm.

6) Will support normal operation -

The CFMS will provide plant data for normal operation as well as abnormal or emergency conditions.

7) Display some additional parameters

The CFMS displays parameters at a system level (core, primary system, etc.), and at the subsystem or component level (valves, pumps, etc) in order to give a detailed view.

8) Integrate with emergency procedures

Efforts have been completed to integrate the CFMS use with emergency procedures.

A. Design Of Displays

Display design criteria of the San Onofre Nuclear Generating Station CFMS took the following into account:

Detectability - brightness, size, contrast & glare

Perceptability - symbols, scales & graphic forms

Interpretability - meaning

Density - clutter

The main objective of the graphics displays is to assist the operator in making correct decisions in an optimal way during all conditions. With that objective in mind, the displays were designed to be simple and easy to understand; callup of a new display would be rapid; and effective, consistent use of color was incorporated for fast operator response.

A checklist of design considerations in graphics displays included:

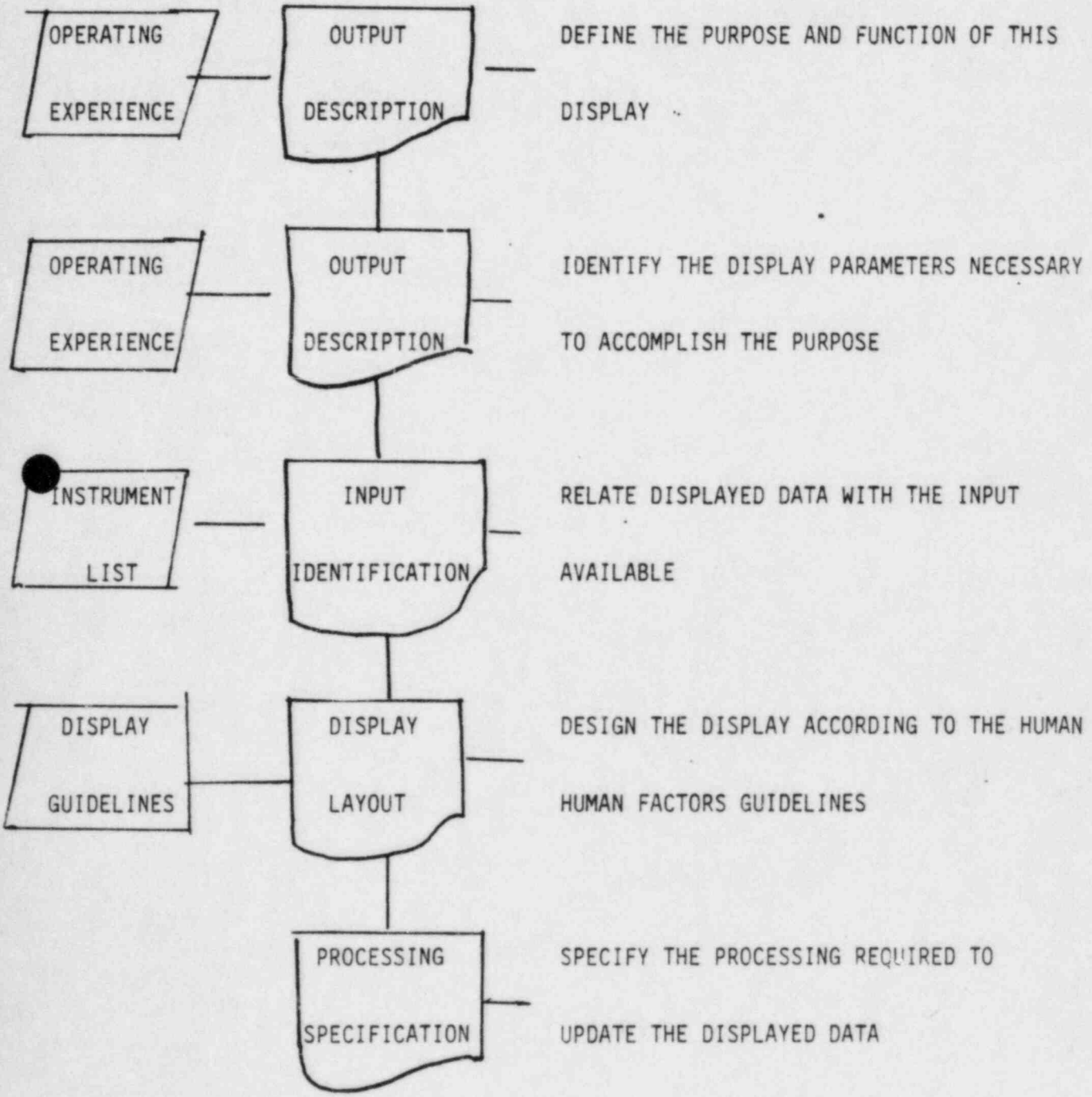
- o Understanding the task the operator performs
- o Identifying what information the operator needs to perform the task
- o Selecting the proper display techniques.

Figure 2 summarizes the display design methodology used for SCE's CFMS.

The CFMS is designed to maximize contrast with hues. For example, the dark background of the CRT and dark blue containing non-essential information contrast with the cyan, yellow and magenta hues used for monitoring and updating. Alphanumerics are scaled not less than the 5 by 7 pixel matrix recommended by good human factors practice (Reference 3). These display designs are consistent with recommendations found in NUREG 0835.

FIGURE 2

DISPLAY DESIGN METHODOLOGY



Only upper case letters are used in the CFMS displays, since studies indicate that upper case letters are more legible than lower case. To ensure legibility, the character height is displayed at a minimum angle of 16 minutes of arc (Reference 4).

Color coding is used to represent information categories on the display screen. In a paper presented to the Instrument Society of America, M. M. Danchek recommended the following color codes:

RECOMMENDED COLOR CODES

COLOR	USE
Black	Display Background
Blue	Non-Essential or Non-Information Bearing Data
Cyan	Essential or Information Bearing Numeric Data or Text
Green	Off, De-Energized, Closed, Normal
Red	On, Energized, Open, Bypassed
White	Intermediate Between Green and Red
Yellow	Cautionary, Attention Required
Magenta	Danger, Immediate Attention Required

The display hierarchy focuses on the concept of how the pages are related according to the operators scheme of the process. The display hierarchy is established by defining the purpose and

function of the display set and each individual display. The hierarchy consists of three levels: See Figure 3.

Level 1 - Overall status

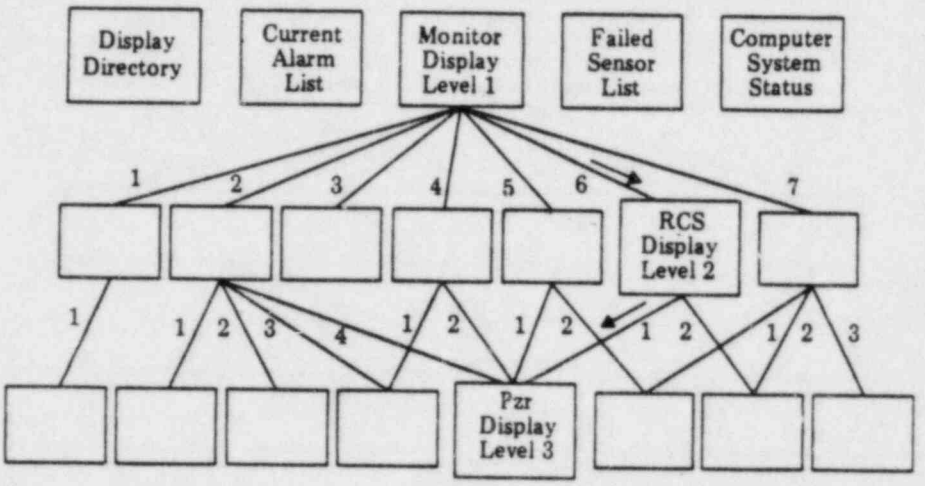
Level 2 - Function status

Level 3 - Subfunction diagnostic

The CFMS display hierarchy was organized on a systems level that dealt with the major systems of the plant, such as the NSSS, main steam, etc., relying heavily on operating experience to meet operator requirements. The three levels are arranged in a tree structure that allows an operator to "zoom in" on problem areas in a rapid, straightforward manner. The hierarchy is designed to be self guiding. The primary advantage is that the information is organized in a structured, spatial and system-oriented fashion. This allows the user to move through the hierarchy with a minimum of key strokes, no dialogs, a minimum of memorization, and no guide books.

FIGURE 3

CFMS DISPLAY HIERARCHY

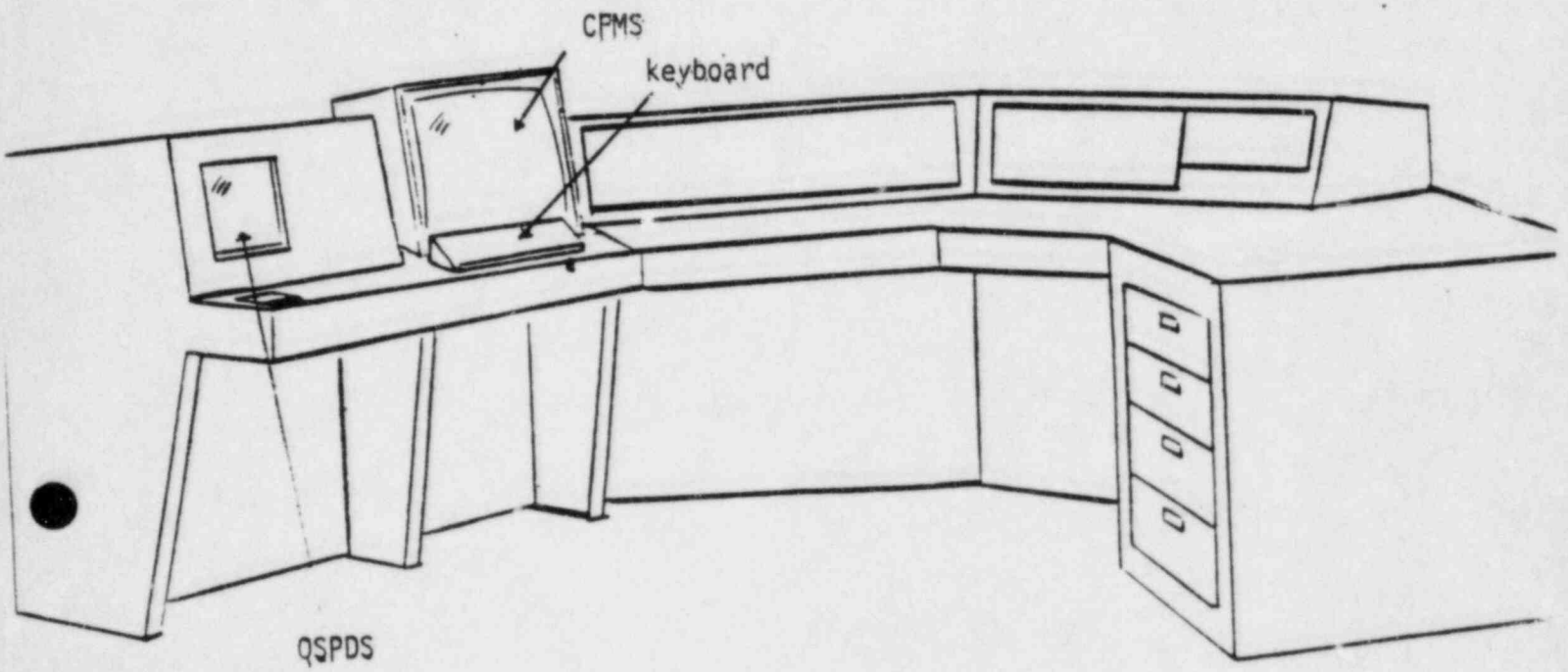


- The display system automatically cues the operator on the occurrence of alarm(s). The sector number and associated symbol will appear in the alarm color, blinking, allowing the operator to follow a structural fault diagnostic path within the display hierarchy.

B. DESIGN OF OPERATOR STATION

The control room at SONGS is relatively compact for each of the Units 2 and 3, affording shift supervisor a good view of the total plant condition. In this context, the control board and CFMS displays are both complementary and interchangeable. Because of the intended use of the SPDS as a supervisory aid, the design of SPDS operator station was appropriately located at operator desks away from the control panels. See Figure 4.

FIGURE 4



SPDS DISPLAY INSTALLATION AT SONGS

C. USER FUNCTIONAL TRAINING:

Comprehensive training in the use and interpretation of the CFMS has been given to operators, plant personnel and management at San Onofre Units 2 and 3 to confirm that the CFMS is readily perceived and comprehended by the SPDS users.

Formal training programs were developed and presented to plant personnel at two separate times. Training was provided by qualified engineers who had taken an INPO-approved instructor training course prior to developing the CFMS course. Recurrent training in the use and interpretation of the CFMS is held at SCE's Training and Educational Center.

III. VERIFICATION AND VALIDATION (V & V)

A. DESIGN VERIFICATION

Verification involves independent requirements review and design review. The requirements are the foundation upon which the SPDS was designed. NUREG-0696 was viewed as the primary requirements for the SPDS. The reviews consisted of evaluating:

1. Determination of human factors requirements for effective man/machine interfacing; these are addressed in Section II.

2. Establishment of the SPDS hardware environment in terms of reliability, maintainability and operating requirements

3. Definition of the inputs, outputs and historical data base requirements

4. Determination of the adequacy of the SPDS alarm strategy in responding to plant emergency conditions in a meaningful fashion.

The objective of the validation testing was to certify that the CFMS operates in accordance with its design specifications. There are two activities with validation testing: 1) Functional and Software Test Plan and 2) test execution and results analysis. (Reference 5).

CFMS test cases were run in order to test the CFMS alarms. The test execution entailed performing the tests, recording the test results and analyzing the results for acceptability. Each test was documented with date, tester, test case, test results and test status.

The level of V & V performed is consistent with the view of the CFMS as a control room operational aid. The SPDS displays plant parameters that monitor the fundamental safety functions.

B. VALIDATION TESTING

1. Algorithm simulator testing

Transient data, generated using standard transient analysis codes were input to the CFMS, and a determination of the appropriate critical function alarms and sequence of alarm was made for dynamic testing purposes. Expected alarms for each jeopardized critical function were observed.

The critical function alarm algorithms were tested using test cases that simulated CFMS inputs. Evaluation of the

test cases and expected results were consistent. These critical function alarm algorithm tests are included as part of the overall CFMS functional test.

2. Halden Reactor Project:

The experimental validation of the critical function monitoring system was carried out by the Halden Project as a joint effort among C-E, the Technical Research Center of Finland (VIT), and Imatran Vorma OY (IVO). The experiments took place at the PWR training simulator situated at the IVO Loviisa Nuclear Power Plant in Finland. The purpose was to assess the impact of the CFMS on operator performance when handling serious plant disturbances. The CFMS project, which lasted more than 18 months, covered all essential details, initial planning, development of a CFMS training program, specification and installation of data recording equipment, practical

training of operating crews, experimentation and data collection, data processing, analysis and evaluation. An effective modular tape-slide training program was used for initial instruction.

The subjects were twelve crews of experienced operators from the nuclear power plant undergoing their semi-annual retraining at the simulator. The experiments, which employed a "within group comparison" design, made substantial use of both video and audio recordings, in addition to computer derived measurement. Two transients were developed which presented the operators with two equivalent, severe and complex plant disturbance scenarios.

The analyses combined quantitative and qualitative methods, and used a detailed timeline description as the

basis for answering questions about the impact of the CFMS. In terms of overall quantitative analysis, two specific hypotheses were investigated:

(1) that operators using the CFMS would maintain critical functions more effectively, and

(2) that effective maintenance of critical functions was equivalent to improved plant safety.

Both the overall results and the more detailed, qualitative investigation of timeline data supported these hypotheses. In addition, the CFMS project demonstrated successfully the methodology developed at Halden.

One description of the overall crew performance was based on a quantitative analysis of measured operator and plant performance factors. The CFMS use could not, however, have been measured in any detail

without the use of the video camera in the control room. (Figure 5) The visual record provided data about which of the operators was using the display and the recorded verbal exchanges between crew members revealed a great deal on information about how they employed the CFMS in response to the transient.

Clearly, the operating crews did use the CFMS to obtain useful information during the test transient. The supervision used the display the most and derived the most benefit from it.

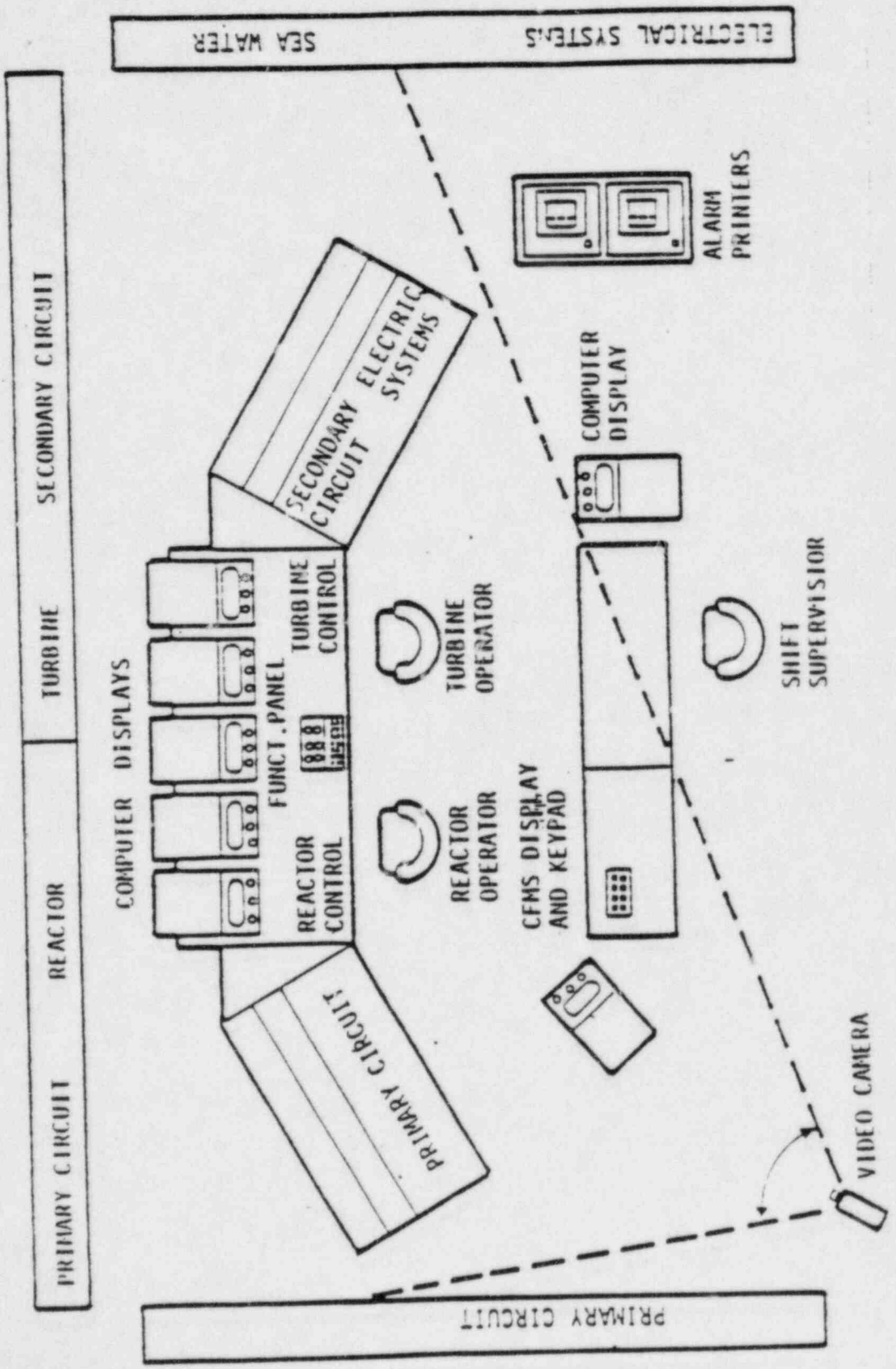
C. CFMS TESTING

1. System Testing

All the functions of the CFMS are fully tested using a functional test procedures document. (Reference 5) The

Figure 5

HALDEN PROJECT VALIDATION SETUP



functional tests include input processing, alarm state transition tests, display processing, annunciator output tests, inadequate core cooling tests, and others. All test exceptions are identified, resolved, and the function retested before CFMS software is delivered to the site. An independent review of this testing process is also performed.

2. Pre-operational Testing

Pre-operational testing is performed at San Onofre, before the CFMS software is officially installed for use by control room operators. Pre-operational testing includes all of the functional testing mentioned in the previous section, as well as hardware tests and string checks. This provided not only a check on the software, but a check on the installed system.

IV. COMPARISON OF CFMS TO NUREGs

IV. A. NUREG 0696

	Requirement	CFMS Compliance
1)	Provide an SPDS available during normal operation and during all classes of emergencies.	1) The CFMS is designed to display the safety status of the plant during all modes of operation and for normal and all emergency conditions.
2)	Should provide information on a) reactivity control b) reactor core cooling and heat removal from the primary system c) reactor coolant system integrity d) radioactivity control e) containment integrity	2) See Section I.B.3.
3)	The unavailability of the SPDS shall be 0.01 (availability > 0.99) when reactor is above cold shutdown. The cold shutdown unavailability shall be 0.2. For additional 0696 requirements, See Section IV.D on NUREG-0835	3) CFMS and QSPDS designed to achieve availability > 0.99.

IV. B. NUREG 0737

Requirement	CFMS Compliance
1) Reactor vessel level indication	1) QSPDS, CFMS provide indication of reactor vessel level.
2) Indication of Inadequate Core Cooling (ICC) should determine the existence of inadequate core cooling caused by various phenomena.	2,3) Indication of ICC is independent of the initiating event.
3) ICC indication should be unambiguous.	
4) Provide advance warning of ICC.	4) Advance warning of ICC is provided by saturation margin calculation, reactor vessel level calculation and core exit thermocouple temperature.
5) Cover full range from normal operation to complete core uncovery.	5) Saturation margin, reactor vessel level, and core exit thermocouple temperature are displayed at all times. Reactor vessel level is measured to the top of the core. Core exit thermocouples provide indication of the trend of cladding temperature in the core.
6) Core exit thermocouple-primary displays	6)
a) core map available on demand	a) Core maps are available on demand
b) selective reading of core exit temperature	b) Representative core exit temperature, which is a conservatively high core exit temperature, is displayed and trended.
c) direct readout hard copy capability available for all thermocouples	c) thermocouple temperatures displayed on a core map which can be called up on demand with hard copy printout available.
d) temperature range from 200° to 1800 (at least)	d) temperature range for thermocouples is 32°F to 2300°F.

IV. B. NUREG 0737 (Continued)

	Requirement		CFMS Compliance
	e) trending of representative core exit temperature available on demand.		e) representative core exit temperature trend available on CFMS on demand.
	f) alarm capability		f) alarm generated if representative CET temperature exceeds a setpoint
	g) operator display device interface should be human factored.		g) CFMS displays are human factored in accordance with NUREG 0835.
7)	Backup display should provide reading of at least 16 operable thermocouples, 4 per quadrant in at least 6 minutes; range should be from 200°F to 2300°F.	7)	QSPDS provides 56 core exit thermocouple temperatures, 14 per quadrant. The display is on a core map which is available on demand. The thermocouple range is from 32° to 2300°F.
8)	Primary, backup display channels should be electrically independent, powered from 1E power sources, physically separate, up to the isolation devices.	8)	1E inputs to the primary SPDS (CFMS) are isolated. 1E inputs to the backup display (QSPDS) are not isolated since the QSPDS is a 1E system. The inputs are electrically and physically separate.
9)	Beyond isolation device, primary SPDS need not be class 1E, but energized from a high reliability power source which is battery backed.	9)	The CFMS is powered from a high reliability power source which is battery backed.
10)	Backup display and associated hardware should be class 1E.	10)	The QSPDS is a 1E system.
11)	Primary, backup display channels should provide 99% availability to display 4 thermocouples per quadrant (also in NUREG-0696).	11)	The CFMS and QSPDS are designed to achieve 99% availability.

IV. C. NUREG 0737 Supplement 1

	Requirement		CFMS Compliance
1)	SPDS is a concise display of critical plant variables to the control room operators, used to evaluate safety status of the plant.	1)	The CFMS is a data acquisition and display system in the control room which presents essential plant information useful in diagnosing the safety status of the plant.
2)	SPDS should function during normal, abnormal and emergency conditions.	2)	The CFMS is intended for use in normal abnormal and emergency conditions.
3)	SPDS should be located convenient to the control room operators.	3)	The CFMS is located in the control room.
4)	SPDS shall be suitably isolated from electrical or electronic interference with equipment and sensors used in safety systems.	4)	CFMS inputs from the QSPDS or from 1E systems are isolated.
5)	Shall be designed according to accepted human factors principles.		See Section II.
6)	Should provide information to plant operators on:		See Section I.B. 3
	a) reactivity control b) reactor, core cooling and heat removal from the primary system.		
	c) reactor coolant system integrity		
	d) radioactivity control		
	e) containment (integrity)		

IV. D. NUREG 0835

General Acceptance Criteria	CFMS Compliance
1) Primary SPDS display contains sufficient information from which the operator can assess plant safety status.	1) See Section I.B.
2) Operators must be trained on the use of the SPDS.	2) See Section II.C.
3) Display of abnormal operating conditions should be different than the display during normal operating conditions.	3) CFMS uses color changes and flashing to alert the operator of a change in status.
4) Time history of parameters for at least 30 minutes should be displayed.	4) The operator selects the time scale for trends.
5) Parameter magnitudes should be displayed so that the operator recognizes change from normal conditions.	5) Parameter ranges are chosen such that the operator recognizes the change from normal to abnormal conditions, and from abnormal to emergency conditions.
6) Parameter magnitudes should be scaled to allow tracking over a wide range of abnormal conditions.	6) Operator selects the ranges on parameter trends.
7) Each parameter should be labeled for identification.	7) Each parameter is labeled with an identifier, magnitude or status.
8) Colors should conform to NUREG-0700, Sect. 6.5.1.6 or 6.7.2.7.	8) Normal indication - light blue, "caution" indication - yellow, "danger" indication - magenta.
9) No more than 2 levels of severity when there is a parameter change in status.	9) See above.
10) Symbols, mimics; see NUREG-0700, Sect. 6.6.3.4, 6.6.6.4.	10) Standard symbols shape codes indicate major components for the operational displays and critical function status.

IV. D. NUREG 0835 (Continued)

General Acceptance Criteria	CFMS Compliance
11) Overlays should not interfere with observation or interpretation of plant operating conditions.	11) The CFMS does not use overlays.
12) Setpoints for display changes should be chosen based on technical considerations.	12) Hi and lo setpoints (yellow) were chosen to alert the operator to deviation from normal conditions. Hi-hi and lo-lo setpoints were chosen to alert the operator to an approach to safety limits.
13) Blinking, flashing conform with NUREG-0700, Sect. 6.3.3.2 and 6.7.2.7.	13) Blinking and flashing are used to alert the operator of new alarms.

NUREG 0696 Sections
As Interpreted By
NUREG 0835

0696 Requirement		CFMS Compliance
1) Primary Function The primary function of the SPDS is to serve as an operator aid in the rapid detection of abnormal conditions by providing a display of plant parameters from which the safety status of operation may be assessed in the control room.	(NUREG 0696 Sections) 5.1 1.3.4	
0835 Interpretation This criterion is satisfied when:		
a) the primary SPDS display format contains functional information to assist the operator in rapidly evaluating the safety status of the plant.		a) the SPDS provides information on the operability and status of plant systems required for safety.
and b) abnormal conditions which impact safety of the plant are easily identified and recognized from the primary SPDS display format.		b) the occurrence of parameter and critical function alarms are shown on every display page.
and c) the SPDS supplements the control room annunciator system when severe plant transients occur.		c) An alarm on the plant annunciator occurs when a critical function alarm occurs.

0696 Requirement		CFMS Compliance
2) Secondary Functions The display system may include other functions that aid operating personnel in evaluating plant status. Secondary functions, such as the performance monitoring of plant systems or safety systems and the presentation of data to assist the operator to diagnose abnormal operating conditions may be used. No acceptance criteria for the secondary functions were specified in 0835.	(NUREG 0696 #5.5)	
0835 Interpretation The secondary functions are acceptable provided: a) They do not impair the operator's use of the SPDS in executing the primary function. and b) the control room operating crew has been trained in the use of the secondary functions.		a) secondary displays are used to support the primary SPDS displays. b) control room personnel have received functional training on the SPDS and how to operate SPDS displays.
0696 Requirement		
3) Future Functions The design of the display system should be flexible to allow for future incorporation of advanced diagnostic concepts and evaluation techniques and systems.	(0696 Section #5.5)	

	0835 Interpretation		CFMS Compliance
	The criterion may be satisfied in designs using a computer based system when either:		
	a) the design is expandable to accept new functions.		a) the SPDS has capability to upgrade to 1) Larger CPU 2) More main memory 3) Additional bulk memory 4) multi-processing-parallel processing
	or b) the design allows for the addition of processors, memories or additional computers, such as in a distributed network.		
	0696 Requirement		
4)	Basis of Parameter Selection	0696 Section 5.5	
	The basis for selection of the minimum set of parameters in the primary display shall be documented as part of the design.		
	0835 Interpretation		
	This criterion is satisfied when: it can be demonstrated that the primary display format, using the parameters selected meets the guidelines or criteria of Section 3 of 0835.		See Section 1.B.
	0696 Requirement		
5)	Real Time Validation	0696 Section 5.1	
	Display data shall be validated on a real time basis where practicable.		

0835 Interpretation	CFMS Compliance
This criterion is satisfied by:	
a) comparing redundant sensor readings prior to the display of the parameter.	a1) *out of range points denoted by ?? and identified on the Failed Sensor Listing.
or	
b) using analytical redundancy among different parameters and using models and equations that have been documented and validated. Operating regimes were the equations used are not valid should be identified and documented.	a2) comparison of CFMS variables with corresponding points from other sources (plant computer and vertical board) conducted by the operator on a regular basis for real-time validation.

0696 Requirement

6) Unvalidated Data — 0696 Section 5.1

Display data which is unvalidated shall be so indicated to operators.

0835 Interpretation	CFMS Compliance
This criterion is satisfied when:	
a) validated parameters, unvalidated parameters, and invalid data are identified, where practical	a) unvalidated data may be taken out of scan
and	
b) validated parameters are coded in a manner whereby they are easily distinguished from unvalidated parameters.	b,c) unvalidated parameters displayed on the CFMS are clearly distinguishable from validated parameters.
and	
c) coding of invalid data is distinct from the coding of data for which data validation is unsuccessful.	

0835 Interpretation	CFMS Compliance
and d) operating procedures for use of the SPDS provides guidance for treatment of invalid data and resolution of unsuccessful data validation.	d) Procedures exist to take invalid data out of scan.
and e) operator training in the use of the SPDS includes practice in dealing with unvalidated data and application of procedures to resolve unsuccessful data validation.	e) operators are trained on taking unvalidated data out of scan.

Operator knowledge of the validity of data is important in correctly assessing the safety status of the plant.

0696 Requirements

7) Design Principles — 0696 Section 5.5

The display format shall be designed to accepted human factors principles.

0835 Interpretation

This criterion is satisfied when:

a) the design conforms to the display guidelines presented in NUREG 0700,	a) See Section II
and b) the primary display format conforms to the general criteria in Section 3 of 0835.	b) See Section II

0696 Requirement		CFMS Compliance
8) Individual Parameters The primary display may be a continuous indication of individual plant parameters or may be composed of a number of measured variables or derived variables.	0696 Section 5.1 5.5	
0835 Interpretation This criterion is satisfied when:		
a) a dedicated display, such as a CRT, with a single primary display format continuously displays the minimum parameter set necessary to assess the safety status of the plant.		a) The critical function display page displays all the algorithms used in assessing the safety status of the plant.
or b) reduction in size of the primary display format is provided when it is necessary to display secondary information.		b) The critical function matrix is displayed on all other display pages in the lower left. When an alarm occurs in a critical function algorithm, the critical function matrix will flash. This prompts the operator to return to the critical function display page for further assessment.

	0696 Requirement	0696 Section	CFMS Compliance
9)	Timeliness and Accuracy of Data Displayed data shall present current and accurate status of the plant. 0835 Interpretation The criterion is satisfied when:	5.1	
	a) the sampling rate for each parameter is chosen such that there is no meaningful loss of information in the data presented to the operator.		a) The CFMS display is updated every 1 second
	and b) the time delay from when the sensor signal is sampled to when it is displayed is no greater than 2 seconds.		b) Time delay is less than 2 seconds.
	and c) maintaining the control room SPDS display is given processor priority over display and processing requests from the TSC, EOF, or other sources.		c) All displays are given equal priority except that the control room has priority in setting up HDSR trends.
	and d) each parameter is displayed with an accuracy sufficient for the operator to discriminate between abnormal conditions which impact safety and normal operating conditions.		d) CFMS alarms exist for the algorithms to alert the operator of deviation from normal conditions (hi or low alarms), and of the approach to safety limits (hi-hi and lo-lo alarms)

	0696 Requirement		CFMS Compliance
10)	Scope of Data The display should be responsive to transient and accident sequences. 0835 Interpretation The criterion is satisfied when: a) operator comprehension of a change in the safety status of the plant from the primary SPDS display could be achieved in a matter of seconds. If closure of this task takes several minutes, the design is unacceptable. and b) the display system correctly portrays the plant process status for all design basis events and events specified by NUREG-0737, Section I.C.1, Guidance For The Evaluation and Development of Procedures For Transients and Accidents	0696 Section 5.5	a) The CFMS display is updated every 1 second. b) See Section III
11)	Parameter Grouping Parameters must be grouped to enhance operators assessment of the plant and to assist in making functional comparisons.	0696 Section 5.1	

0835 Interpretation		CFMS Compliance
This criterion is satisfied when:		
a)	the minimum set of parameters are presented on the single primary display format. The minimum set of parameters must be the ones by which the operator evaluates the safety status of the plant.	a) The critical function display page shows minimum set of plant parameters necessary to determine the safety status of the plant.
and		
b)	the parameters displayed are grouped so that all are visible to the operator within one field of view.	b) The critical function display page shows each critical function and the algorithm legs that comprise each critical function.
and		
c)	the parameters are sequenced in a logical manner to facilitate operator comparison of parameters in evaluating the safety status of the plant.	c) The CFMS uses a top down display hierarchy where the first level displays plant overview information, the second level shows algorithm Systems information and the third level shows subsystem and component information.
and		
d)	the primary display format utilizes patterns and display enhancements as discussed in Section 3 of 0835.	d) Patterns and display enhancements are discussed in Section II and in this Section.

0696 Requirements		0696 Section
12)	Pattern and Coding Pattern and coding techniques shall be used to assist operator detection and recognition of unsafe operating conditions.	5.1

0835 Interpretation	CFMS Compliance
This criterion can be satisfied by:	
a) the use of color coding to indicate the approach to unsafe operation and to indicate unsafe operation.	a) The CFMS utilizes color changes and flashing to alert the operator of an approach to unsafe operation.
or	
b) the use of limit marks for each parameter displayed. The limit marks should be representative of operational limits established by technical specifications, process limits, and safety system actuation setpoints, if applicable.	
or	
c) the use of patterns which noticeably distort when an unsafe condition is approached.	

0696 Requirement	0696 Section
13) Magnitude, Trend	5.1
The display shall be capable of presenting magnitudes and trends of parameters or derived variables. The display of time derivatives in lieu of trends may be acceptable.	

0835 Interpretation	CFMS Compliance
This criterion is satisfied when:	
a) the primary display format contains the magnitude for all variables being displayed.	a) The magnitude of all variables and the status of all pumps and valves are continuously displayed.
and	
b) the primary display format has the capability of indicating trends, or trends of operator selected parameters are available in a secondary display format.	b) The operator has the capability to select trends.
and	
c) trend data is displayed with sufficient resolution in time and magnitude to ensure that rapidly changing parameters are accurately displayed. The frequency bandwidth of the signal measurement system, consisting of sensor, signal processing devices and trend display device should be broad enough to transmit all meaningful information of the measured parameter or derived variable.	c) The operator selects the range and time scale over which a parameter trend may be observed.
The display of time derivatives of variables is acceptable only when the derivatives unambiguously reflect the trends in the variables. The algorithm used for time derivatives must be adequate to track oscillating plant variables that may exist during the design basis events for the plant.	

	0696 Requirement	0696	CFMS Compliance
14)	Recall Capabilities	Section 5.5	
	The recall of additional data on secondary formats or displays is desirable.		
	0835 Interpretation		
	This criterion is met when:		
	a) operator requests to the display system will result in displays, of additional data, on secondary formats, such as trend data of the safety status parameters.		a) The operator can display secondary pages by direct paging, sectoring down through the hierarchy or by paging forward or backwards.
	and		
	b) data is available for retrieval and is not lost as a result of an electrical power failure.		b,c) Data is available from disk or magnetic tape which is loaded by computer operators. The CFMS power supply has high reliability.
	and		
	c) data stored for retrieval is stored on a secure medium and is available upon demand.		
	and		
	d) response times to operator requests for information on secondary displays conforms with NUREG-0700 guidelines for computer response time to operator queries.		d) The response time for operator requested displays is designed to be less than 5 seconds.
	0696 Requirement		
15)	Mode of Plant Operation	0696 Section 5.5	
	The design of the display shall contain a single primary display format for each mode of plant operation.		

0835 Interpretation	CFMS Compliance
This criterion is satisfied when:	
a) the design contains a primary display format for each mode of plant operation defined by the technical specifications of operation.	a) The display format is the same for all operating modes. The CFMS is designed to monitor the plant safety status during all modes of operation.

A common display format composed of the same parameters may be used for several modes of plant operation. However, for any one mode, the display must contain that minimum set of parameters needed to assess the safety status of the plant.

Typical modes of plant operation are:

1. Power Operation
2. Startup
3. Hot Standby
4. Hot Shutdown
5. Cold Shutdown
6. Refueling

0696 Requirement

16) Display Format Selection — 0696 Section 5.5

For each plant operating mode, display formats may either be automatically displayed or manually selected.

0835 Interpretation

This criterion is satisfied when:

a) a manually operated switch or input from an alpha-numeric keyboard, touch panel, light pen, cursor, or equivalent interface is provided by the design to allow the operator to adjust the display format for the mode of plant operation.	a) display can be selected by using an alphanumeric keyboard.

	0835 Interpretation		CFMS Compliance
	or b) an automatic display format change occurs with a change in mode of plant operation.		
	0696 Requirement		
17)	Display Location The SPDS shall be located in the control room with additional displays provided in the TSC and EOF.	0696 Section 5.2	
	0835 Interpretation		
	This criterion is satisfied when: provisions are made for locating the SPDS display and associated controls in the control room, TSC, and EOF.	1)	The SPDS displays an keyboards are located in the control room, TSC, and EOF.
	0696 Requirement		
18)	Control Board If the SPDS is part of the control board, it must be easily recognizable and readable.	0696 Section 5.2	
	0835 Interpretation		
	This criterion is satisfied when: a) the SPDS is readily distinguished from other displays on the control board. and b) the display conforms to the appropriate display readability guidelines stated in NUREG 0700.	a) b)	The SPDS displays are separate from the control panel. Display format is discussed herein.

	0696 Requirement	0696	CFMS Compliance
19)	Display Readability	Section 5.3	
	The display shall be readable from the emergency station of the Senior Reactor Operator.		
	0835 Interpretation		
	This criterion is satisfied when:		
	a) the displays design conforms to the appropriate display readability guidelines stated in NUREG-0700, such as viewing distance, viewing angle, and screen location for standing and seated operators at the Senior Reactor Operator's Station.		a) CRT located at 2/3 CR-66 operating desk of SRO.
	and		
	b) the data displayed on the CRT's has acceptably low flicker and noise.		b) CRT used has low flicker and noise.
	and		
	c) Alpha-numeric characters generated with a 7 x 9 dot matrix or larger are preferable; characters with 5 x 7 dot matrix are acceptable, if necessary.		c) characters do not have less than a 5 x 7 dot matrix.
	and		
	d) density of display is less than 25% when complex symbology e.g. mimics are displayed.		d) Display density is not greater than 40%
	and		
	e) for ease of detection, acceptable symbol to background contrast ratio should fall in a range of 3:1 to 4:1. for all important data.		e) CFMS symbols are well highlighted and distinguishable from background

		CFMS Compliance
	and	
f)	motion of data displayed on a CRT to prevent screen burnout is at a rate slow enough to avoid distracting the operator.	f) See b)

0696 Requirement

		0696
20)	Display Accessibility	Section 5.2

The display shall be readily accessible and visible to the:
Shift Supervisor
Control Room Senior Reactor Operator
Shift Technical Advisor
One Reactor Operator.

0835 Interpretation

This criterion is satisfied when:

a)	physical obstructions do not block a person's field of view when the person is at the normal work station.	a) no physical obstruction, CRT and plasma display inset low in new operating consoles.
and		
b)	if the SPDS is not in the operator's direct field of view at the workstation, a reorientation of his/her field of view allows viewing the SPDS from the workstation.	b) CRT visible from seated position (Figure 3)
and		
c)	members of the control room operating crew have physical access to the SPDS from their normal workstation. For example, a short direct walk to the SPDS is acceptable.	c) CRT part of operators desk
and		
d)	glare from normal or emergency lighting does not restrict viewing of the SPDS from within the control room. The use of antiglare techniques and devices are acceptable when they are in accord with other criteria stated in this report.	d) anti gloss CRT screens used

			CFMS Compliance
	and e) luminance levels and luminance contrast do not limit viewing from locations throughout control room.		e) CRT adjustable locally for maximum visibility
	0696 Requirement		
21)	Control Accessibility The display system shall not interfere with the normal movement of the control room operation crew. The display system shall not interfere with full visual access to other control room operating systems and displays.	0696 Section 5.3	
	0835 Interpretation		
	This criterion is satisfied when:		
	a) the display system does not obstruct the normal movement of the control room operating crew.		a) CRT does not obstuct the normal movement of the operator
	and b) the display system does not interfere with the full visual access to other control room operating systems and displays.		b) CRT does not obstruct the visual access to the other control room systems and displays
	0696 Requirement		
22)	Control Room Staff No additional operating staff other than the normal control room operating staff should be needed for operation of the display.	0696 Section 5.4	

0835 Interpretation	CFMS Compliance
This criterion is satisfied when:	
a) no additional operating staff other than the normal control room operating staff need be added for operation of the SPDS.	a) Operators are trained on operations of SPDS
and b) the operator training program contains instructions on the use of the SPDS.	b) Operator training on functional use of the SPDS includes instructions on use.
and c) an SPDS user's manual is available for operator reference in the control room.	c) Users manual available in the control room.
and d) interaction with and SPDS computer is designed such that training in computer programming is not required.	d) Operator can call up displays, perform all historical data storage and reset alarms from the alphanumeric keyboard.

0696 Requirement

23) Operator Interaction — 0696 Section 5.5

Flexibility to allow for interaction by the operator is desirable in the design of the display designs.

0835 Interpretation

The criterion is satisfied when:

a) the system contains operator interactive devices.	a,b,c) Each display station has an alpha-numeric keyboard with 11 (eleven) function keys that allow the operator to manipulate displays set up historical data storage and retrieval tasks, acknowledge and reset alarms. Positive identification of operator
b) the display system positively acknowledges each request that the design allows the operator to make.	

	0835 Interpretation	CFMS Compliance
	c) system response times to operator request conform to the guidelines of NUREG 0700. Undue time delays in response to a request are unacceptable.	requests can be observed from display changes. Response times are designed to be less than 5 seconds.

Function keys for the recall of data are the preferred type of interactive devices. Keyboards are acceptable for use in the recalling of data provided the necessary syntax is simple and straightforward to use. Alpha-numeric keyboards added to SPDS should have the same keyboard layout as other keyboards in control room. Other interactive devices such as touch panels or light pens may also be acceptable.

0696 Requirement

		0696 Section
24)	Failure Recognition	5.6

The control room operations staff shall be provided with sufficient information and criteria for performance of an operability evaluation of the SPDS.

0835 Interpretation

This criterion may be satisfied by:

a)	designing a monitoring system in the display which may be automatic or operator activated.	a) There are a number of software and hardware diagnostics within the CFMS that will alert the operator to hardware or software failures.
or		
b)	a display of calendar date and time of day, with some means of indicating the passage of seconds. The display should be updated only when the system is operating properly so that	b) The CFMS has the current time displayed within 5 seconds on each display page.

0835 Interpretation	CFMS Compliance
a static time would indicate a system failure. The data and time should be located in a corner of the display so as not to distract the operator.	
or	
c) the operable status of the display system is available upon operator demand.	
or	
d) An equivalent means of evaluating display system operability is available.	

0696 Requirement

		0696
25)	Technical Specification	Section 5.6

A technical specification of operations is required to define compensatory measures for the operator when the SPDS is inoperable.

0835 Interpretation

This criterion is satisfied when:

a) the technical specification defines acceptable compensatory measure for each function performed by the SPDS.

a) no technical specifications exist on SPDS, however QSPDS is a seismic qualified backup display system

The use of the seismic qualified back-up display, monitored on a frequent basis, may be an acceptable compensatory measure. The same minimum set or comparable set of safety status parameters on the SPDS primary display format should be present on the backup. Also, the backup display must be readily interpretable by the operator.

	0696 Requirement	0696 Section	CFMS Compliance
26)	Audible Alarms	5.5	
	Where feasible, the SPDS should include some audible notification to alert personnel of an unsafe operating condition.		
	0835 Interpretation		
	This criterion is met when:		
	a) the display system emits a distinct audible sound, such as the beeper available on computer terminals, upon detecting an abnormal operating condition.		a) The CFMS provides an output for critical function alarms for the plant annunciator.
	and		
	b) the SPDS alarm system has provisions to silence, acknowledge, reset and test these functions, as appropriate.		b) The CFMS keyboard will acknowledge all visual alarms on the display. The plant annunciator system has the capability to acknowledge and reset the audible alarm.
	An audible alarm from the SPDS need not meet the intensity requirements given in NUREG-0700.		
	SPDS alarms should be independent of the annunciator system and should not result in the generation of the same audible alarms as the annunciator system.		
	0696 Requirement		
27)	Functional Qualification	0696 Section 5.1	
	A functional qualification program should be established to demonstrate SPDS operational conformance with the functional design criteria.		

0835 Interpretation	CFMS Compliance
This criterion is satisfied when:	
a) a test plan is available for the display system. The test plan shall define a minimum of one test case for each major functional criterion of the display system. The object of the test case is to illustrate the correct performance of the implemented design.	a) A test plan exists for the CFMS that tests all major functions of the SPDS (reference 5).
and	
b) a test report containing the results of the test cases is compiled. All major functional criteria must be tested successfully.	b) A test report was completed based on the the plan in a) above
and	
c) all display formats in the design are tested, including mode dependent formats.	c) displays are given human factors considerations. There are no mode dependent formats.
and	
d) a human factors review of the SPDS in accordance with appropriate portions of NUREG-0700 is performed with results evaluated in accordance with the guidelines presented in NUREG 0801. The results of this effort are to be documented by the licensee/ applicant as part of the control room design review.	d) for human factors considerations, see Section II.
and	
e) a trained control room operating crew can effectively use the SPDS to detect abnormal plant operating conditions which impact safety.	e) Control room operating crew has received functional training on the use of the CFMS.

	0696 Requirement	0696 Section 5.6	CFMS Compliance
28)	Backup Displays Displays designated as a seismically qualified backup to the SPDS must be designed to accepted human engineering principles. 0835 Interpretation This criterion is satisfied when:		
	a) the back-up displays contain the same minimum set of safety status parameters as presented in the primary display format of the SPDS or an equivalent comparable set of safety status parameters.		a) The backup SPDS display, the QSPDS, displays a smaller, but similarly organized set of 1E inputs vital to plant safety.
	and b) the back-up display is capable of operating during and following earthquakes, to the same degree as control room displays needed to comply with Regulatory Guide 1.97.		b) The backup display has been seismically qualified from sensor through the display.
	and c) the needed seismically qualified displays are concentrated into one segment of the control board. Dependence on poorly human-engineered Class 1E seismically qualified instruments that are scattered throughout the control room is not acceptable.		c) All of the backup SPDS parameters are available on 2 redundant displays (2).
	and d) the backup displays, when reviewed as a group, conform with the guidelines of NUREG-0700.		d) Human factors considerations have been incorporated into QSPDS design.

			CFMS Compliance
	and e) meters on the control board which are part of the SPDS backup display are readily identified and are not likely to be confused with similar meters in the vicinity.		e) Displays are separate from the control board.
	0696 Requirement		
29)	Primary Display, Seismically Qualified	0696 Section 5.6	
	It is preferred that only one display system be used for evaluating the safety status of the plant. However, an alternative is to design the overall SPDS function with a primary and a backup display.		
	0835 Interpretation		
	When the option for a seismically qualified primary display is selected, this option is satisfied when:		
	a) the design of the primary display conforms to Regulatory Guide 1.97, Revision 2, December 1980. "Instrumentation For Plants to Assess Plant and Environs Conditions During and Following An Accident"		a) This option not implemented.
	and b) the design conforms to the acceptance criteria defined in this report, with the exception of the context of Section 28, Backup Displays.		

V. SAFETY ANALYSIS ITEMS

1. The safety parameter display system is electrically isolated from all other safety systems. All inputs are wired through analog and digital chassis cabinets, and the CFMS operates on its own power supply. Thus, the CFMS would not degrade any other safety related system.

2. The SPDS serves as a backup for main control board information during normal conditions, and as such would only confirm indications in the control room. The CFMS would not provide any misleading information that could not be confirmed on the main control board, and therefore confuse an operator to take inappropriate action.

3. The SPDS contains approximately 1000 points; and with the exception of composed points, all the inputs can be confirmed through other instrumentation.

4. The SPDS will not pose a safety hazard; it is a passive, monitoring and indication system only, and does not interfere with the automatic initiation of any protection system.

5. The CFMS contains the five critical safety functions of Supplement 1 to NUREG-0737. The correlation between the eight critical functions of the CFMS and the 5 safety functions listed in Supplement 1 is discussed in section 1.B.3.

REFERENCES

(1) L. P. Goodstein and J. Rasmussen, "Man-Machine System Design Criteria in Computerized Control Rooms," proceedings of ASSOP080, IFIP/IFAC Symposium, Trondheim, Norway, June, 1980.

(2) Yankee Atomic Electric Company, "Verification and Validation of the Yankee Plant Safety Parameter Display System", Nuclear Safety Analysis Center/61, January, 1984.

(3) M. M. Danchak, "Alphanumeric Displays for the Man-Process Interface," Combustion Engineering TIS-5301, Windsor, CT.

(4) M. M. Danchak, "The Man-Process Interface Using Computer Generated CRT Displays," ISA Power Symposium, New Orleans, LA, May, 1977.

(5) Functional Test Procedures for San Onofre Nuclear Generating Station-CFMS, 1470-ICE_4503, Rev. 03.

(6) W. R. Corcoran, et.al., "The Operators Role and Safety Functions," Workshop on Licensing and Technical Issues, Washington, D.C., March 1980.